ABUS Security Tech Germany

eyseo.ip

TVIP40000

Ⓓ **Bedienungsanleitung**

Ⓔ **User manual**

Ⓕ **Manuel utilisateur**

ⓃⓁ **Gebruikershandleiding**

ⒹⓀ **Brugerhåndbog**

Version 10/2010

CE

Deutsch

**Diese Bedienungsanleitung enthält wichtige Hinweise zur Inbetriebnahme und Handhabung.
Achten Sie hierauf, auch wenn Sie dieses Produkt an Dritte weitergeben.
Heben Sie deshalb diese Bedienungsanleitung zum Nachlesen auf!**

Eine Auflistung der Inhalte finden Sie im Inhaltsverzeichnis mit Angabe der entsprechenden Seitenzahlen auf **Seite 3.**

English

**These user manual contains important information for installation and operation.
This should be also noted when this product is passed on to a third party.
Therefore look after these operating instructions for future reference!**

A list of contents with the corresponding page number can be found in the index on **page 59**.

Français

Ce mode d'emploi appartient à de produit. Il contient des recommandations en ce qui concerne sa mise en service et sa manutention. Veuillez en tenir compte et ceci également lorsque vous remettez le produit à des tiers. Conservez ce mode d'emploi afin de pouvoir vous documenter en temps utile!

Vous trouverez le récapitulatif des indications du contenu á la table des matières avec mention de la page correspondante á la **page 119**.

Nederlands

**Deze gebruiksaanwijzing hoort bij dit product. Er staan belagrijke aanwijzingen in betreffende de ingebruikname en gebruik, ook als u dit product doorgeeft aan derden.
Bewaar deze hendleiding zorgvuldig, zodat u deze later nog eens kunt nalezen!**

U vindt een opsomming van de inhoud in de inhoudsopgave met aanduiding van de paginanummers op **pagina 175 .**

Dansk

Denne manual hører sammen med dette produkt. Den indeholder vigtig information som skal bruges under opsætning og efterfølgende ved service. Dette skal huskes også når produkter gives videre til anden part. Læs derfor denne manual grundigt igennem også for fremtiden.

Indholdet kan ses med sideanvisninger kan findes i indekset på **side 232**

Deutsch

ABUS
Security Tech Germany

eyseo.ip

TVIP40000

Bedienungsanleitung

Version 10/2010

Originalbedienungsanleitung in deutscher Sprache. Für künftige Verwendung aufbewahren!

Einführung

Sehr geehrte Kundin, sehr geehrter Kunde,

wir bedanken uns für den Kauf dieses Produkts.

Dieses Produkt erfüllt die Anforderungen der geltenden europäischen und nationalen Richtlinien. Die Konformität wurde nachgewiesen, die entsprechenden Erklärungen und Unterlagen sind beim Hersteller (www.abus-sc.com) hinterlegt.

Um diesen Zustand zu erhalten und einen gefahrenlosen Betrieb sicherzustellen, müssen Sie als Anwender diese Bedienungsanleitung beachten!

Lesen Sie sich vor Inbetriebnahme des Produkts die komplette Bedienungsanleitung durch, beachten Sie alle Bedienungs- und Sicherheitshinweise!

Bei Fragen wenden Sie sich an ihren Facherrichter oder Fachhandelspartner!

Haftungsausschluss

Diese Bedienungsanleitung wurde mit größter Sorgfalt erstellt. Sollten Ihnen dennoch Auslassungen oder Ungenauigkeiten auffallen, so teilen Sie uns diese bitte auf der Rückseite des Handbuchs angegebener Adresse mit.
Die ABUS Security-Center GmbH übernimmt keinerlei Haftung für technische und typographische Fehler und behält sich das Recht vor, jederzeit ohne vorherige Ankündigung Änderungen am Produkt und an den Bedienungsanleitungen vorzunehmen.
ABUS Security-Center ist nicht für direkte und indirekte Folgeschäden haftbar oder verantwortlich, die in Verbindung mit der Ausstattung, der Leistung und dem Einsatz dieses Produkts entstehen. Es wird keinerlei Garantie für den Inhalt dieses Dokuments übernommen.

Symbolerklärung

Das Symbol mit dem Blitz im Dreieck wird verwendet, wenn Gefahr für die Gesundheit besteht, z.B. durch elektrischen Schlag.

Ein im Dreieck befindliches Ausrufezeichen weist auf wichtige Hinweise in dieser Bedienungsanleitung hin, die unbedingt zu beachten sind.

Dieses Symbol ist zu finden, wenn Ihnen besondere Tipps und Hinweise zur Bedienung gegeben werden sollen.

Wichtige Sicherheitshinweise

Bei Schäden die durch Nichtbeachten dieser Bedienungsanleitung verursacht werden, erlischt der Garantieanspruch. Für Folgeschäden übernehmen wir keine Haftung!

Bei Sach- oder Personenschäden, die durch unsachgemäße Handhabung oder Nichtbeachten der Sicherheitshinweise verursacht werden, übernehmen wir keine Haftung. In solchen Fällen erlischt jeder Garantieanspruch!

Sehr geehrte Kundin, sehr geehrter Kunde, die folgenden Sicherheits- und Gefahrenhinweise dienen nicht nur zum Schutz Ihrer Gesundheit, sondern auch zum Schutz des Geräts. Lesen Sie sich bitte die folgenden Punkte aufmerksam durch:

- Es sind keine zu wartenden Teile im Inneren des Produktes. Außerdem erlischt durch das Öffnen/Zerlegen die Zulassung (CE) und die Garantie/Gewährleistung.
- Durch den Fall aus bereits geringer Höhe kann das Produkt beschädigt werden.
- Dieses Gerät ist für den Betrieb im Innenbereich vorgesehen.
- Für den Betrieb im Außenbereich verwenden bitte Sie ein geeignetes Schutzgehäuse.

Vermeiden Sie folgende widrige Umgebungsbedingungen bei Betrieb:

- Nässe oder zu hohe Luftfeuchtigkeit
- Extreme Kälte oder Hitze.
- Direkte Sonneneinstrahlung
- Staub oder brennbare Gase, Dämpfe oder Lösungsmittel
- starke Vibrationen
- starke Magnetfelder, wie in der Nähe von Maschinen oder Lautsprechern.
- Der Videoserver darf nicht auf unbeständigen Flächen installiert werden.

Allgemeine Sicherheitshinweise:

- Lassen Sie das Verpackungsmaterial nicht achtlos liegen! Plastikfolien/-tüten, Styroporteile usw., könnten für Kinder zu einem gefährlichen Spielzeug werden.
- Der Videoserver darf aufgrund verschluckbarer Kleinteile aus Sicherheitsgründen nicht in Kinderhand gegeben werden.
- Bitte führen Sie keine Gegenstände durch die Öffnungen in das Geräteinnere
- Verwenden Sie nur die vom Hersteller angegebenen Zusatzgeräte/Zubehörteile. Schließen Sie keine nicht kompatiblen Produkte an.
- Bitte Sicherheitshinweise und Bedienungsanleitungen der übrigen angeschlossenen Geräte beachten.
- Überprüfen Sie vor Inbetriebnahme das Gerät auf Beschädigungen, sollte dies der Fall sein, bitte das Gerät nicht in Betrieb nehmen!
- Halten Sie die Grenzen der in den technischen Daten angegebenen Betriebsspannung ein. Höhere Spannungen können das Gerät zerstören und ihre Sicherheit gefährden (elektrischer Schlag).

Sicherheitshinweise

1. Stromversorgung: Netzteil 110-240 VAC, 50/60 Hz **/** 12VDC, 1.5 A (im Lieferumfang)
   Betreiben Sie dieses Gerät nur an einer Stromquelle, die die auf dem Typenschild angegebene Netzspannung liefert. Falls Sie nicht sicher sind, welche Stromversorgung bei Ihnen vorliegt, wenden Sie sich an Ihr Energieversorgungsunternehmen. Trennen Sie das Gerät von der Netzstromversorgung, bevor Sie Wartungs- oder Installationsarbeiten durchführen.

2. Überlastung
   Vermeiden Sie die Überlastung von Netzsteckdosen, Verlängerungskabeln und Adaptern, da dies zu einem Brand oder einem Stromschlag führen kann.

3. Reinigung
   Reinigen Sie das Gerät nur mit einem feuchten Tuch ohne scharfe Reinigungsmittel.
   Das Gerät ist dabei vom Netz zu trennen.

Warnungen

Vor der ersten Inbetriebnahme sind alle Sicherheits- und Bedienhinweisung zu beachten!

1. Beachten Sie die folgende Hinweise, um Schäden an Netzkabel und Netzstecker zu vermeiden:
   - Verändern oder manipulieren Sie Netzkabel und Netzstecker nicht.
   - Verbiegen oder verdrehen Sie das Netzkabel nicht.
   - Wenn Sie das Gerät vom Netz trennen, ziehen Sie nicht am Netzkabel, sondern fassen Sie den Stecker an.
   - Achten Sie darauf, dass das Netzkabel so weit wie möglich von Heizgeräten entfernt ist, um zu verhindern, dass die Kunststoffummantelung schmilzt.

2. Befolgen Sie diese Anweisungen. Bei Nichtbeachtung kann es zu einem elektrischen Schlag kommen:

   - Öffnen Sie niemals das Gehäuse oder das Netzteil.
   - Stecken Sie keine metallenen oder feuergefährlichen Gegenstände in das Geräteinnere.
   - Um Beschädigungen durch Überspannungen (Beispiel Gewitter) zu vermeiden, verwenden Sie bitte einen Überspannungsschutz.

3. Bitte trennen Sie defekte Geräte sofort vom Stromnetz und informieren Ihren Fachhändler.

Vergewissern Sie sich bei Installation in einer vorhandenen Videoüberwachungsanlage, dass alle Geräte von Netz- und Niederspannungsstromkreis getrennt sind.

Nehmen Sie im Zweifelsfall die Montage, Installation und Verkabelung nicht selbst vor, sondern überlassen Sie dies einem Fachmann. Unsachgemäße und laienhafte Arbeiten am Stromnetz oder an den Hausinstallationen stellen nicht nur Gefahr für Sie selbst dar, sondern auch für andere Personen.
Verkabeln Sie die Installationen so, dass Netz- und Niederspannungskreise stets getrennt verlaufen und an keiner Stelle miteinander verbunden sind oder durch einen Defekt verbunden werden können.

Auspacken

Während Sie das Gerät auspacken, handhaben sie dieses mit äußerster Sorgfalt.

Bei einer eventuellen Beschädigung der Originalverpackung, prüfen Sie zunächst das Gerät. Falls das Gerät Beschädigungen aufweist, senden Sie dieses mit Verpackung zurück und informieren Sie den Lieferdienst.

Inhaltsverzeichnis

Bestimmungsgemäße Verwendung

Eine ausführliche Funktionsbeschreibung finden Sie im Kapitel „4. Erstinbetriebnahme“.

Das Produkt darf nicht feucht oder nass werden. Der Videoserver ist nur für den Einsatz in trockenen Räumen vorgesehen.

Eine andere Verwendung als oben beschrieben kann zur Beschädigung des Produkts führen, außerdem bestehen weitere Gefahren. Jeder andere Einsatz ist nicht bestimmungsgemäß und führt zum Verlust der Garantie bzw. Gewährleistung; sämtliche Haftung wird ausgeschlossen. Dies gilt auch, wenn Umbauten und/oder Veränderungen am Produkt vorgenommen wurden.

Lesen Sie sich die Bedienungsanleitung vollständig und aufmerksam durch, bevor Sie das Produkt in Betrieb nehmen. Die Bedienungsanleitung enthält wichtige Informationen für Montage und Bedienung.

1. Lieferumfang

ABUS D1 Videoserver H.264

Netzadapter

Montagematerial

Kurzanleitung

Software CD
inklusive Bedienungsanleitung

2. Montage

Stellen Sie sicher, dass im Lieferumfang alle Zubehörteile und Artikel, die auf der vorherigen Liste aufgeführt sind, vorhanden sind. Für den Betrieb des Videoservers ist ein Ethernet-Kabel erforderlich. Dieses Ethernet-Kabel muss den Spezifikationen der UTP-Kategorie 5 (CAT 5) entsprechen und darf eine Länge von 100 Metern nicht überschreiten.

2.1 Stromversorgung

Bevor Sie mit der Installation beginnen, stellen Sie sicher, dass die Netzspannung und die Nennspannung des Videoservers übereinstimmen.

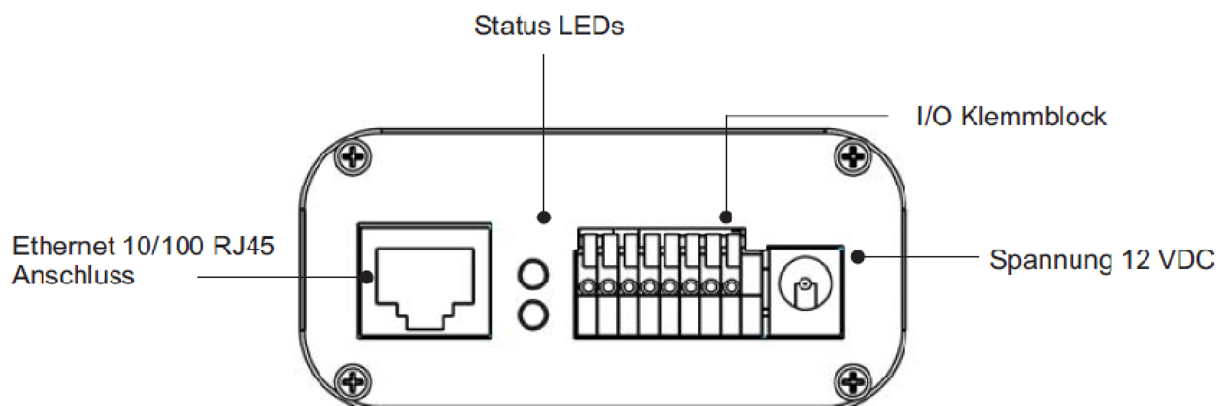
2.2 Montieren des Videoservers

Für die Wandmontage des Videoservers werden die im Lieferumfang befindlichen Haltebügel und Schrauben benötigt.

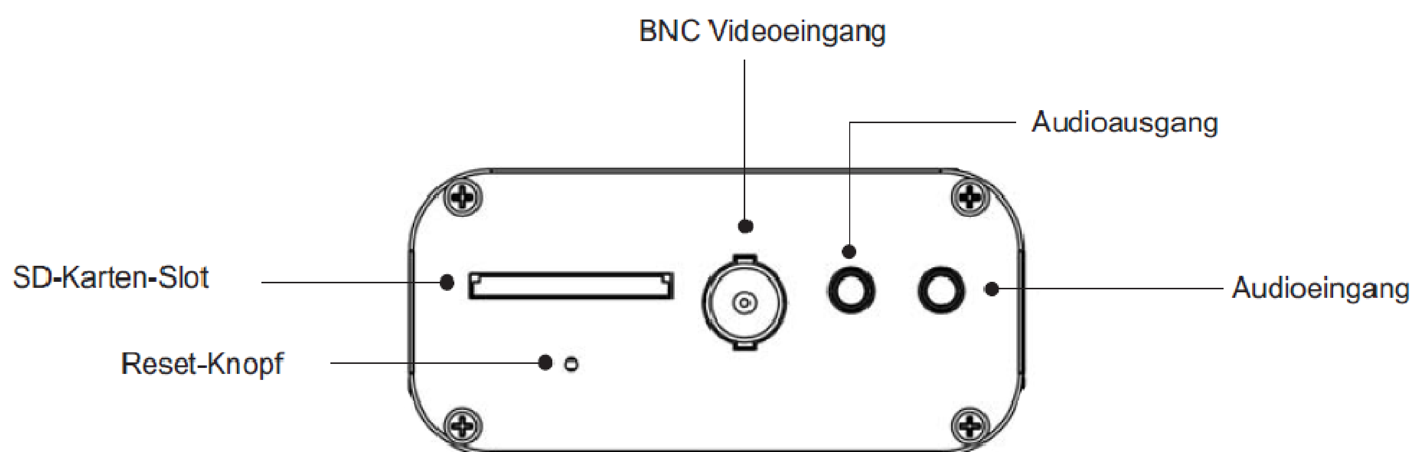
ACHTUNG!
Während der Montage muss der Videoserver von der Netzspannung getrennt sein.

3. Beschreibung des Videoservers

3.1 Vorderansicht

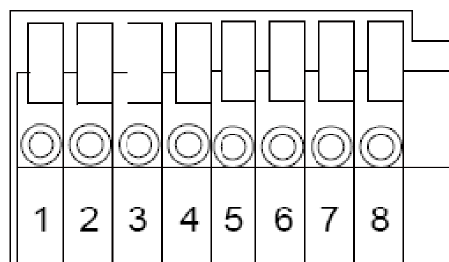


3.2 Rückansicht

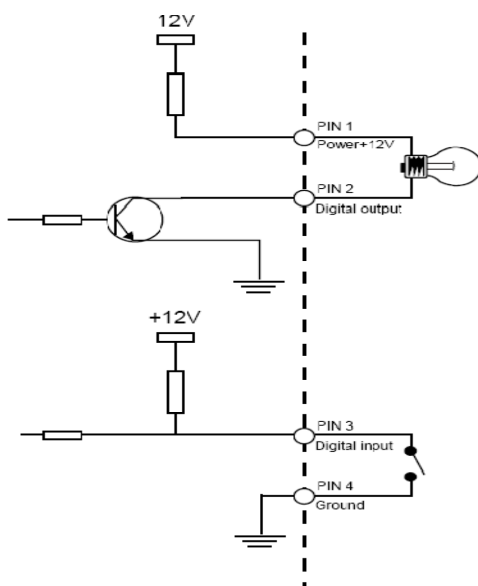


3.3 Alarmeingänge und Relaisausgänge

PIN	Beschreibung
1	+12V Ausgang
2	Schaltausgang
3	Alarmeingang
4	Masse
5	24V AC Eingang
6	24V AC Eingang
7	RS-485 +
8	RS-485 -



3.4 Schaltein-/ausgang und Statusanzeige



Blinkcode Status LED

Zustand / LED Farbe	Grün	Rot
Systemstart	An	An
Ausgeschaltet	Aus	Aus
Netzwerk bereit	1/s	An
Netzwerkproblem	Aus	An
Während Firmware Upgrade	1/s	0.1/s
Werkseinstellungen setzen	0.1/s	0.1/s

Nutzen Sie die **Reset**-Taste, um die Einstellungen des Videoservers auf den Auslieferungszustand zurückzusetzen oder um den Videoserver manuell neu zu starten. Benutzen Sie hierzu ein entsprechend schmales Werkzeug.

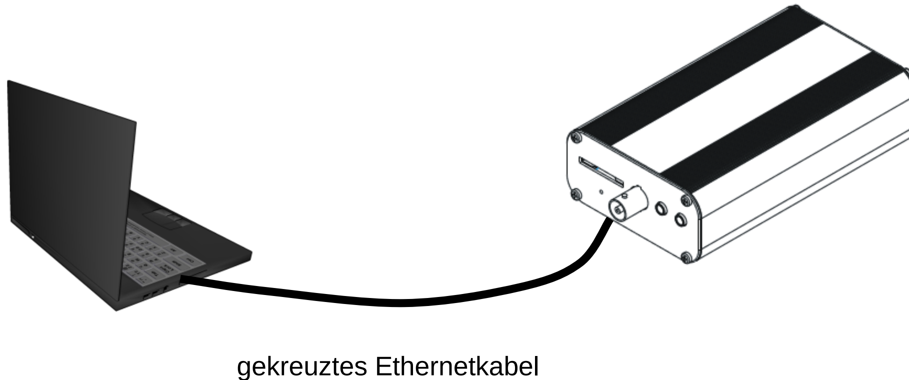
Videoserver **neu starten:** Drücken Sie die Reset-Taste einmalig und warten Sie bis der Videoserver wieder betriebsbereit ist.

Videoserver zurücksetzen: Drücken Sie die Reset-Taste dauerhaft für ca. 30 Sekunden bis die Status LEDs zu blinken beginnen. Alle Einstellungen im Videoserver werden auf den Auslieferungszustand zurückgesetzt.

4. Erstinbetriebnahme

Direkter Anschluss des Videoservers an einen PC / Laptop

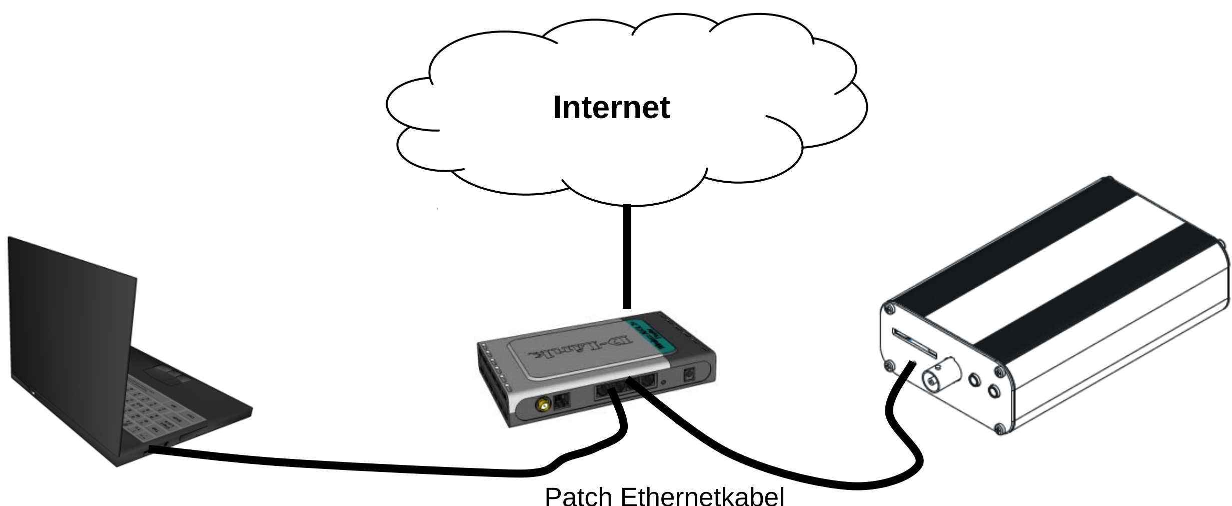
1. Stellen Sie sicher, dass Sie ein gekreuztes Netzwerkkabel (Cross-Over) benutzen.
2. Verbinden Sie das Kabel mit der Ethernet-Schnittelle des PCs / Laptop und des Videoservers.
3. Schließen Sie die Spannungsversorgung des Videoservers an.
4. Konfigurieren Sie die Netzwerkschnittelle Ihres PCs / Laptop auf die IP Adresse 169.254.0.1
5. Gehen Sie weiter zu Punkt 4.1, um die Ersteinrichtung abzuschließen und die Verbindung zum Videoserver aufzubauen.



gekreuztes Ethernetkabel

Anschluss des Videoservers an einen Router / Switch

1. Stellen Sie sicher, dass Sie ein Patch-Kabel für die Vernetzung benutzen.
2. Verbinden Sie den PC / Laptop mit dem Router / Switch.
3. Verbinden Sie den Videoserver mit dem Router / Switch.
4. Schließen Sie die Spannungsversorgung des Videoservers an.
5. Wenn in Ihrem Netzwerk ein Namensserver (DHCP) verfügbar ist, dann stellen Sie die Netzwerkschnittstelle Ihres PCs / Laptop auf „IP Adresse automatisch beziehen“. Sollte kein Namensserver (DHCP) verfügbar sein, konfigurieren Sie die Netzwerkschnittelle Ihres PCs / Laptop auf 169.254.0.1.
6. Gehen Sie weiter zu Punkt 4.1, um die Ersteinrichtung abzuschließen und die Verbindung zum Videoserver aufzubauen.



Patch Ethernetkabel

4.1 Erster Zugang zum Videoserver

Der erste Zugang zum Videoserver erfolgt unter Verwendung des Installationsassistenten 2.
Nach dem Start des Assistenten sucht dieser nach allen angeschlossenen EyseoIP Netzwerkkameras und Videoservern in Ihrem Netzwerk.

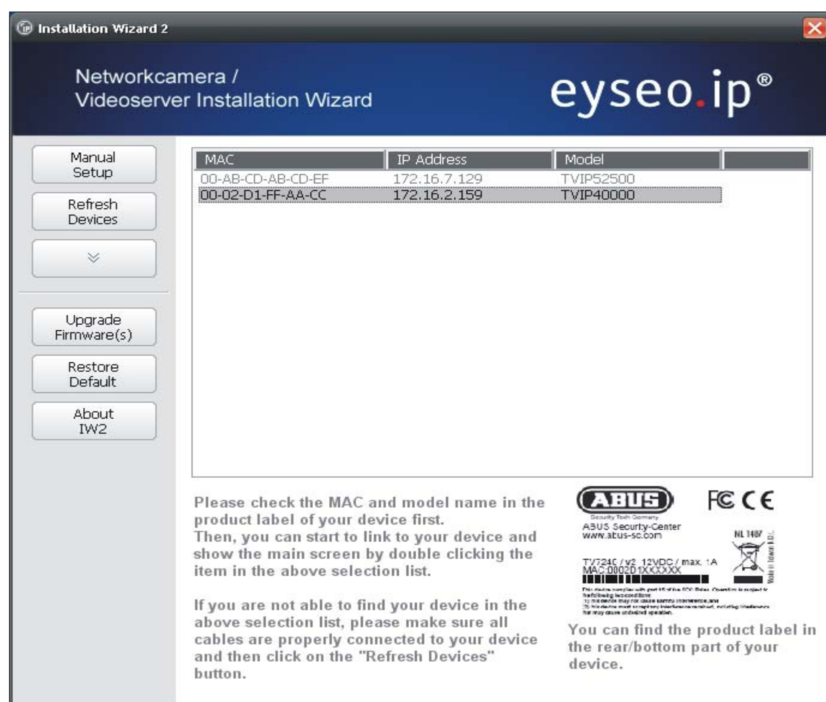
Sie finden das Programm auf der beiliegenden CD-ROM unter: **CD-ROM\Tools\EyseoIP Tools**

Installieren Sie das Programm auf Ihr PC-System und führen Sie es aus. Der Installlationsassisten2 sucht automatisch nach EyseoIP-Videoservern in Ihrem Netzwerk.

Die Standard IP-Adresse des Videoservers lautet **169.254.0.99**. Ohne Verwendung des Installationsassistenten können Sie direkt auf den Videoserver zugreifen, wenn Ihr PC-System auf folgenden Adressbereich konfiguriert ist 169.254.0.1- 169.254.0.98.

Falls ein DHCP-Server in Ihrem Netzwerk vorhanden ist, erfolgt die Vergabe der IP-Adresse sowohl für Ihren PC / Laptop, als auch den Videoserver automatisch.

Starten Sie jetzt den Installationsassistenten. Ist kein DHCP-Server verfügbar, fügt der Installationsassistent eine virtuelle IP Adresse aus dem Bereich 169.1254.0.xx zu Ihrer TCP/IP-Konfiguration hinzu. Solange der Installationsassistent geöffnet ist, können Sie über diese virtuelle IP-Adresse einen Netzwerkzugriff zum Videoserver aufbauen. Wir empfehlen Ihnen, umgehend die Netzwerkkonfiguration des Videoservers an das Netzwerk, in dem der Videoserver verwendet werden soll, anzupassen.



Nach Beendigen des Installationsassistenten 2 wird die zusätzliche virtuelle IP-Adresse wieder entfernt. Ist die ursprüngliche IP-Adresse des PC-Systems nicht im selben IP-Bereich wie die des IP-Videoservers ist ein Zugriff nicht mehr möglich.

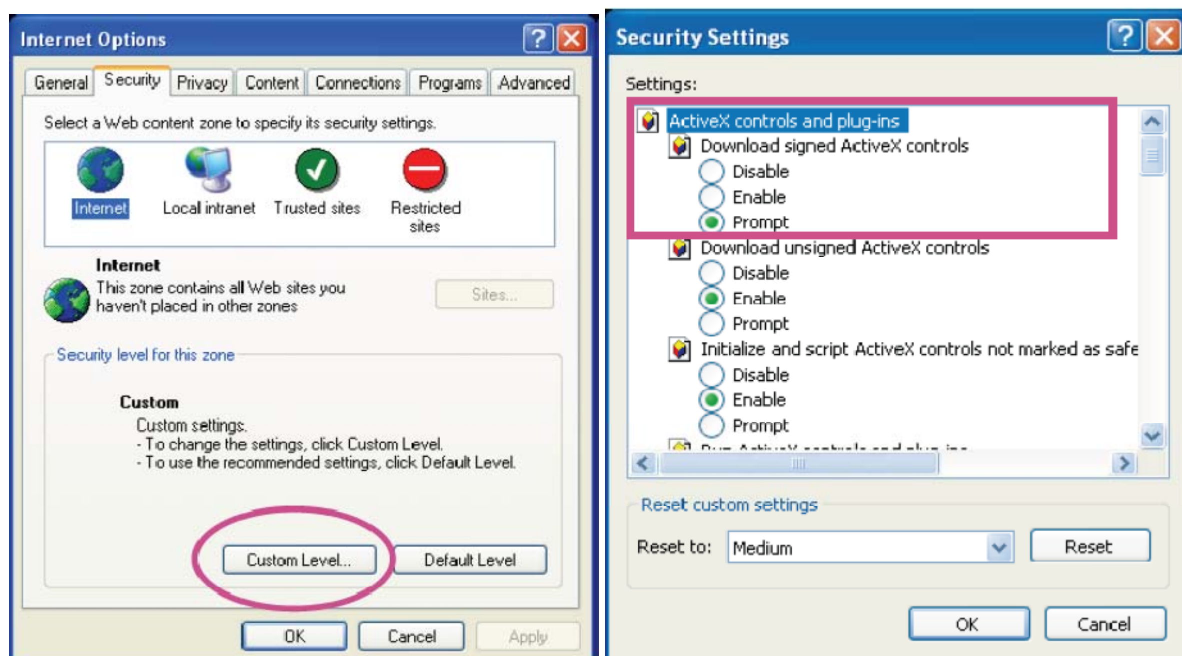
4.2 Zugriff auf den Videoserver mittels Web-Browser

Beim ersten Zugang zum Videoserver unter Windows fragt der Web-Browser nach der Installation eines ActiveX-Plug-Ins für den Videoserver. Diese Abfrage hängt von den Internet-Sicherheitseinstellungen des PC's des Benutzers ab. Falls die höchste Sicherheitsstufe eingestellt ist, kann der Computer jede Installation und jeden Versuch einer Ausführung verweigern. Dieser Plug-In dient zur Videoanzeige im Browser. Zum Fortsetzen kann der Benutzer auf „Installieren" klicken. Lässt der Web-Browser keine Fortsetzung der Installation zu, öffnen Sie die Internet-Sicherheits-Einstellungen und reduzieren Sie die Sicherheitsstufe oder wenden Sie sich an den IT- oder Netzwerk-Administrator.

4.3 Active-X Plugin installieren

Verwenden Sie als Browser Mozilla Firefox oder Netscape um auf Ihren Videoserver zuzugreifen, wird anstatt des AktiveX Plugins ein Quick Time-Stream von dem Videoserver bereitgestellt. Dies setzt voraus, dass Sie Quick Time auf Ihrem Computer installiert haben.

4.4 Sicherheitseinstellungen anpassen



Anmerkung: Es kann dazu kommen, dass die Sicherheitseinstellungen Ihres PC's einen Videostream verhindern. Ändern Sie diese unter dem Punkt „Extras/Internetoptionen/Sicherheit" auf ein niedrigeres Level ab. Achten Sie vor allem darauf, ActiveX Steuerelemente und Downloads zu aktivieren.

4.5 Passwortabfrage

Ab Werk ist in dem Videoserver kein Administratorkennwort vergeben. Aus Sicherheitsgründen sollte der Administrator umgehend ein neues Passwort bestimmen. Nach dem Speichern eines solchen Administrator-Passworts fragt der Videoserver vor jedem Zugang nach dem Benutzernamen und dem Passwort.

Der Benutzername für den Administrator lautet permanent **„root"** und ist nicht zu verändern. Nach dem Ändern des Passworts zeigt der Browser ein Authentifizierungsfenster an und fragt nach dem neuen Passwort. Nach dem Einstellen des Passworts gibt es keine Möglichkeit, das Administrator-Passwort wiederherzustellen. Die einzige Option liegt in der Wiederherstellung sämtlicher werkseitig voreingestellten Parameter.

Für die Eingabe eines Passwortes gehen Sie bitte wie folgt vor:

Öffnen den Internet Explorer und geben Sie die IP-Adresse des Videoservers ein (z.B. „http://192.168.0.99").

Sie werden aufgefordert sich zu authentifizieren:

-> Sie sind nun mit dem Videoserver verbunden und sehen bereits einen Videostream.

4.6 Zugriff auf den Videoserver mittels RTSP Player

Sie haben die Möglichkeit auf die MPEG-4/H.264 Datenströme des Videoservers mit einem RTSP-fähigem Mediaplayer zuzugreifen. Folgende kostenlose Mediaplayer unterstützen RTSP:

- VLC Media Player
- Real Player
- Quicktime Media Player

Das Adressformat für die Eingabe der Verbindungsdaten ist wie folgt aufgebaut:

rtsp://<IP-Adresse des Videoservers>:<rtsp Port>/<Name des Videodatenstroms>

Beispiel
rtsp://192.168.0.99:554/live.sdp

Nähere Informationen finden Sie im Kapitel „RTSP-Übertragung".

4.7 Zugriff auf den Videoserver mittels Mobilfunktelefon

Stellen Sie sicher, dass Sie mit Ihrem Mobilfunktelefon eine Internetverbindung aufbauen können. Eine weitere Voraussetzung ist, dass Ihr Gerät über einen RTSP-fähigen Mediaplayer verfügt. Folgende Mediaplayer für Mobilfunktelefone unterstützen RTSP:

- Real Player
- Core Player

Beachten Sie, dass ein Zugriff mittels Mobilfunktelefon auf den Netzwerkserver nur eingeschränkt, aufgrund einer niedrigen zu erwartenden Netzwerkbandbreite gegeben ist. Wir empfehlen Ihnen daher, folgende Einstellungen für den Video-Stream, um die Datenmenge zu reduzieren:

Video Kompression	MPEG-4
Auflösung	176x144
Schlüsselbildintervall	1 Sekunde
Video Qualität (Konstante Bitrate)	40 Kbit / Sekunde
Audio Kompression (GSM-AMR)	12.2 Kbit / Sekunde

Sollte Ihr Mediaplayer die RTSP-Authentifizierung nicht unterstützen, dann deaktivieren Sie den Authentifizierungsmodus für RTSP in den Konfigurationseinstellungen des Videoservers.

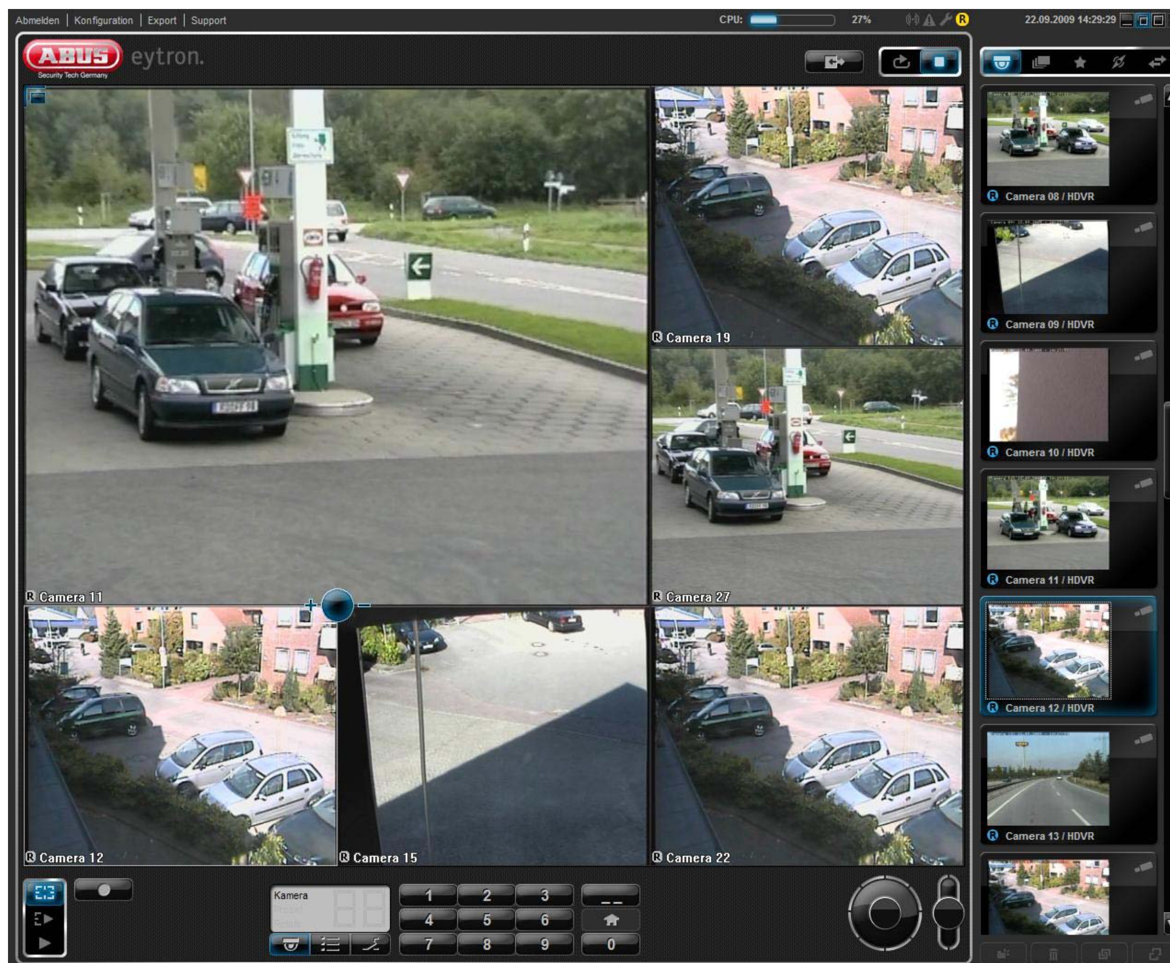
Das Adressformat für die Eingabe der Verbindungsdaten ist wie folgt aufgebaut:

rtsp://<IP-Adresse des Videoservers>:<RTSP Port>/<Name des Videodatenstroms>

Beispiel
rtsp://192.168.0.99:554/live.sdp

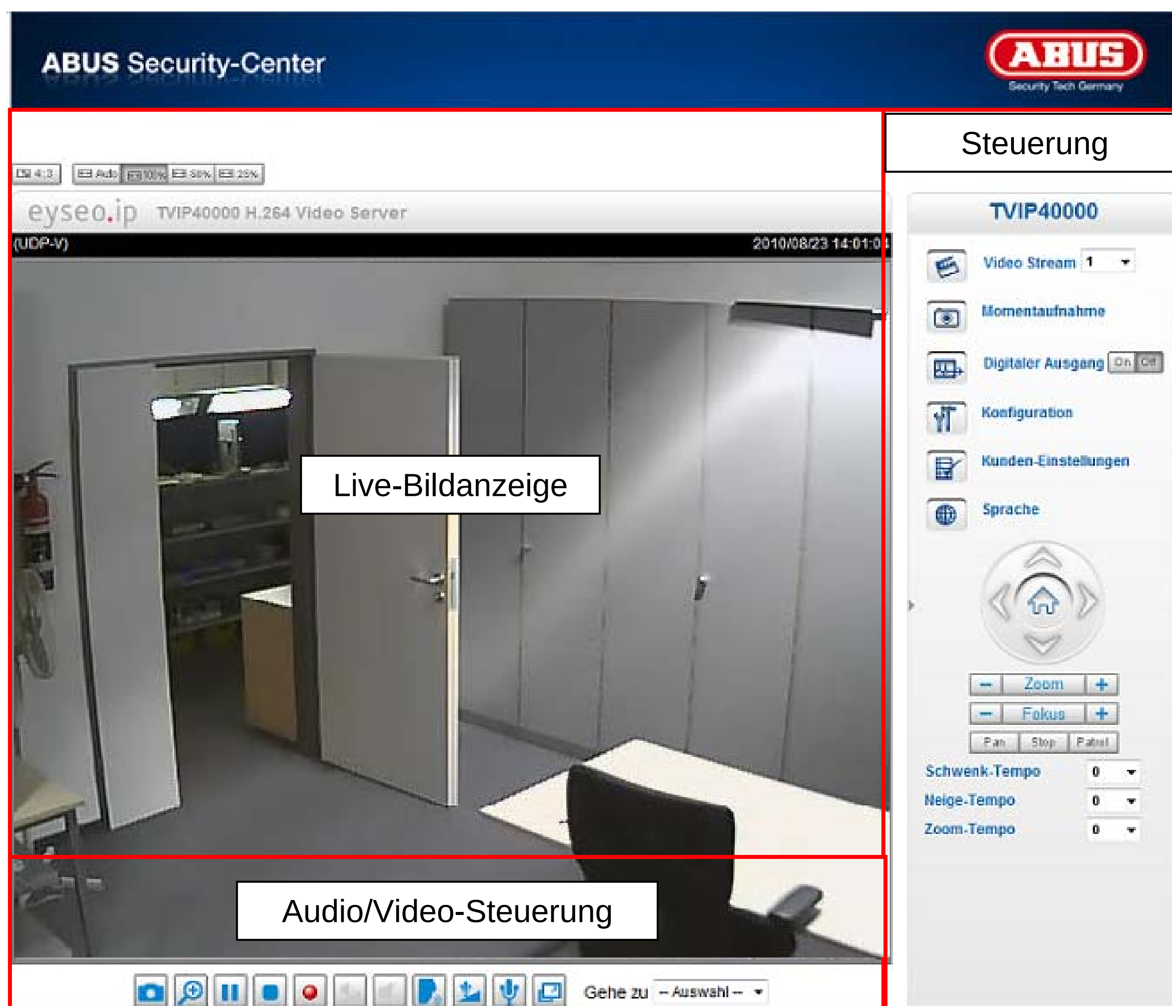
4.8 Zugriff auf den Videoservers mittels eytron VMS Express

Auf der im Lieferumfang enthaltenen CD-ROM finden Sie die kostenlose Aufzeichnungssoftware eytron VMS Express. Hiermit erhalten Sie die Möglichkeit mehrere ABUS Security Center Videoserver über eine Oberfläche einzubinden und Aufzuzeichnen. Weitere Informationen finden Sie im Handbuch der Software auf der beigelegten CD-ROM.



5. Benutzerfunktionen

Öffnen Sie die Startseite des Videoservers. Die Oberfläche ist in folgende Hauptbereiche unterteilt:



Live-Bildanzeige

- Verändern die Zoom-Stufe durch betätigen des Mouse-Scroll-Rades
- Durch einen Klick in das Livebild, können Sie direkt die Steuerung einer analogen Schwenk/Neige-Kamera übernehmen.

Videoserversteuerung

Video Stream

Wählen Sie zwischen Video Stream 1-4 für die Live-Bildanzeige

Momentaufnahme

Erstellen Sie eine Momentaufnahme (ohne ActiveX-Plugin)

Schaltausgang

Schaltausgang manuell Ein- und Ausschalten

Konfiguration

Videoserverkonfiguration durchführen (Administratoreinstellungen)

Kundeneinstellungen

Kundeneinstellungen setzen. Details finden Sie auf den nächsten Seiten.

Sprache

Spracheinstellung der Oberfläche anpassen

PTZ Steuerung

Nutzen Sie die Steuerschaltflächen für digitale und mechanische PTZ Funktion

Angepasste Fenstergröße

Hiermit kann das Livebild in 3 verschiedenen Zoom Stufen (100%, 50% und 25%) angepasst werden. Ebenso ist es möglich das Livebild automatisch an die aktuelle Browsergröße anzupassen. Hierzu muss die Option „AUTO“ angewählt werden.

Bildschirmverhältnis

Mit dem Button „4:3“ wird das Seitenverhältnis des Livebildes auf 4:3 festgelegt.

Menü ein-/ausklappen

Mit dieser Funktion lässt sich die Menüsteuerung ein- und ausklappen.

5.1 Audio/Video-Steuerung

Momentaufnahme

Der Web-Browser zeigt ein neues Fenster an, in dem die Momentaufnahme gezeigt wird. Zum Speichern der Bilddatei auf Ihrem PC, führen Sie einen Rechtsklick auf die Bildfläche aus und wählen die Option „Speichern unter“.

Digitaler Zoom und Momentaufnahme

Klicken Sie auf das Lupen-Symbol unter der Videoserver-Ansicht. Danach erscheint das Bedienfeld für den digitalen Zoom. Deaktivieren Sie das Kontrollfeld „Digitalen-Zoom deaktivieren“ und ändern Sie den Zoomfaktor mit dem Schieberegler.

Start / Stop der Livebildanzeige

Der Live Stream kann wahlweise gestoppt (angehalten) oder beendet werden. In beiden Fällen kann mit dem Play-Symbol der Live Stream fortgesetzt werden.

Lokale Aufnahme

Es kann eine Aufnahme auf die lokale Festplatte gestartet oder gestoppt werden. Der Aufnahmepfad wird unter „Kundeneinstellungen“ konfiguriert.

Lautstärke anpassen

Klicken Sie auf das Symbol, um manuell den Pegel für den Audioausgang einzustellen.

Audio An/Aus

Sprechen

Solange die Schaltfläche gedrückt ist werden Audiosignale vom PC an den Audioausgang des Videoservers übertragen.

Mikrophon Lautstärke

Klicken Sie auf das Symbol, um manuell den Pegel für den Audioeingang des Videoservers anzupassen.

Stumm

Schalten Sie den Audioeingang des Videoservers An/Aus.

Vollbild

Aktivieren Sie die Vollbildansicht. Das Live-Bild des Videoservers wird bildschirmfüllend dargestellt.

5.2 Kunden-Einstellungen

Die Benutzereinstellungen werden auf dem lokalen Computer gespeichert. Es stehen folgende Einstellungen zur Verfügung:

Media-Optionen ermöglicht dem Benutzer die Audio- oder Videofunktion zu deaktivieren.

Protokoll-Optionen ermöglicht die Auswahl eines Verbindungsprotokolls zwischen dem Client und dem Server. Zwei Protokoll-Optionen stehen zur Optimierung der Anwendung zur Verfügung: UDP, TCP, HTTP.

Das UDP-Protokoll ermöglicht eine größere Anzahl Echtzeit Audio- und Videostreams. Einige Datenpakete können dabei jedoch wegen eines starken Datenaufkommens im Netzwerk verloren gehen. Bilder könnten dadurch nur unklar wiedergegeben werden. Das UDP-Protokoll wird empfohlen, wenn keine speziellen Anforderungen gestellt werden.

Im TCP-Protokoll gehen weniger Datenpakete verloren und eine präzisere Videoanzeige wird garantiert. Der Nachteil dieses Protokolls besteht jedoch darin, dass der Echtzeitstream schlechter ist als der des UDP-Protokolls.

Das HTTP-Protokoll wählen Sie, falls das Netzwerk durch eine Firewall geschützt und nur der HTTP-Port (80) geöffnet werden soll.

Die Wahl des Protokolls wird in folgender Reihenfolge empfohlen: UDP – TCP – HTTP

MP4 Aufnahme Optionen: Ermöglicht dem Benutzer den Dateipfad zur Sofortdatenspeicherung anzupassen. Die Schaltfläche „Datum und Uhrzeit an Dateiname anhängen“ erzeugt Dateien mit folgender Kennung:

CLIP_20091115-164403.MP4
Dateiname-Zustatz_JahrMonatTag-StundeMinuteSekunde.MP4

MP4 Aufnahme-Optionen

Ordner: c:\Record Suchen...

Dateiname-Zusatz: CLIP

☑ Datum und Uhrzeit an Dateinamen anhängen

Speichern

Die aufgezeichneten Daten können über einen MP4-fähigen Videoplayer wiedergegeben werden (z.B. VLC Mediaplayer).

6. Administratoreinstellungen

6.1 System

Allein der Administrator hat Zugang zur Systemkonfiguration. Jede Kategorie auf der linken Spalte wird auf den folgenden Seiten erläutert. Die fettgedruckten Texte stellen die spezifischen Angaben auf den Options-Seiten dar. Der Administrator kann die URL unter der Abbildung eingeben, um direkt zur Bildseite der Konfiguration zu gelangen.

ABUS Security-Center

ABUS Security Tech Germany

Konfiguration

- System
- Sicherheit
- HTTPS
- SNMP
- Netzwerk
- DDNS
- Zugangsliste
- Video und Audio
- Bewegungssensor
- Kamera-Sabotageüberwachung
- Kamerasteuerung
- Anwendung
- Aufnahme
- Lokale Speicherung
- Logdatei
- Parameterliste
- Verwaltung

Version: 1210l

Home

System

Hostname: TVIP40000 H.264 Video Server

☐ LED-Anzeige ausschalten

Systemzeit

Zeitzone: GMT+01:00 Amsterdam, Berlin, Rome, Stockholm, Vienna, Madrid, Paris

☐ Sommerzeit aktivieren:

Hinweis: Sie können die Sommerzeiteinstellungen unter Verwaltung speichern oder die Standardwerte verwenden.

◉ Gegenwärtige Angabe für Datum und Uhrzeit beibehalten

○ Mit PC-Zeit synchronisieren

○ Manuell

○ Automatisch

DI und DO

Digitaler Eingang: Normaler Status ist Niedrig ; aktueller Status ist **Hoch**

Digitaler Ausgang: Normaler Status ist Geerdet ; aktueller Status ist **Offen**

Speichern

"**Host-Name**" Der Text zeigt den Titel auf der Hauptseite an.

“**LED-Anzeige ausschalten**” Wählen Sie diese Option, um die LED-Anzeige des Videoservers auszuschalten. Hiermit kann verhindert werden, dass andere Personen den Betrieb des Videoservers feststellen können.

"**Zeitzone**" Paßt die Uhrzeit entsprechend der gewählten Zeitzone an.

„Sommerzeit aktivieren“ Aktiviert die Sommerzeiteinstellungen in dem Videoserver. Es sind bereits alle Sommerzeiteinstellungen für jede Zeitzone in dem Videoserver gespeichert.

"**Gegenwärtige Angabe für Datum und Uhrzeit beibehalten**" Klicken Sie auf diese Option, um das gegenwärtige Datum und die gegenwärtige Uhrzeit des Videoservers zu behalten. Mittels einer internen Echtzeituhr werden das Datum und die Uhrzeit des Videoservers selbst nach einem Spannungsverlust beibehalten.

"**PC-Zeit übernehmen**" Synchronisiert das Datum und die Uhrzeit des Videoservers mit dem lokalen Computer. Das schreibgeschützte Datum und die schreibgeschützte Uhrzeit des PCs werden nach Aktualisierung angezeigt.

“**Manuell**” Stellt das Datum und die Uhrzeit je nach Eingabe durch den Administrator ein. Beachten Sie bei der Eingabe das Format im entsprechenden Feld.

“**Automatisch**” Synchronisiert Datum und Uhrzeit mit dem NTP-Server über das Internet bei jedem Starten des Videoservers. Dies wird nicht gelingen, wenn der zugeordnete Zeit-Server nicht erreichbar ist.

“**NTP-Server**” Ordnet die IP-Adresse oder die Domänenbezeichnung des Zeit-Servers zu. Durch Leerlassen dieses Textkästchens wird der Videoserver mit den Standard-Zeit-Servern verbunden.

„DI und DO“ Stellt den vordefinierten Zustand für Alarmeingang und Relaisausgang ein.

Vergessen Sie nicht, auf **„Speichern“** zu klicken, damit die Änderungen wirksam werden

6.2 Sicherheit

“**Root-Passwort**” Dient zum Ändern des Administrator-Passworts durch das Eingeben des neuen Passworts. Die eingegebenen Passwörter werden aus Sicherheitsgründen nur in Punkten angezeigt. Nach dem Klicken auf „**Speichern**“ fordert der Web-Browser den Administrator auf, das neue Passwort für den Zugang zum Videoserver einzugeben.

“**Benutzer hinzufügen**” Geben Sie den neuen Benutzernamen und das zugehörige Passwort ein und klicken Sie danach auf „**Hinzufügen**“. Der neue Benutzer wird auf der Liste mit den Benutzernamen angezeigt. Insgesamt können zwanzig Benutzerkonten eingerichtet werden.

“**Benutzer editieren**” Öffnen Sie die Liste mit den Benutzernamen, suchen Sie den Benutzer aus, den Sie bearbeiten möchten und verändern Sie die entsprechenden Werte. Klicken Sie auf „**Aktualisieren**“ um die Änderungen zu übernehmen.

“**Benutzer löschen**” Öffnen Sie die Liste mit den Benutzernamen, suchen Sie den Benutzer aus und klicken Sie auf „**Löschen**“, um diesen Benutzer von der Liste zu löschen

Benutzerverwaltung

Administrator: Uneingeschränkter Vollzugriff auf den Videoserver.
Operator: Kein Zugriff auf die Konfigurationsseite. Kann zusätzlich URL-Kommandos ausführen (z.B. PTZ).
Benutzer: Der Zugriff ist auf die Hauptseite (Live-View) beschränkt.

Digitaler Ausgang: Benutzergruppe kann Alarmeingang und Ausgang steuern
PTZ-Steuerung: Benutzergruppe hat Zugriff auf die PTZ-Steuerung
Anonyme Benutzer erlauben: Es findet keine Benutzername- und Passwortabfrage beim Anzeigen der Hauptseite statt.

6.3 HTTPS

Das HTTPS-Protokoll wird zur Verschlüsselung und zur Authentifizierung der Kommunikation zwischen Webserver (Videoserver) und Browser (Client PC) im World Wide Web verwendet. Alle Daten, die zwischen Videoserver und Client-PC übertragen werden sind mittels SSL verschlüsselt. Voraussetzung für HTTPS ist neben der SSL-Verschlüsselung (kompatibel mit allen gängigen Browsern) ein Zertifikat, das die Authentizität der Quelle bestätigt.

„Sichere HTTPS Verbindung aktivieren“ Wahlweise kann ein unverschlüsselter (HTTP) + verschlüsselter (HTTPS) Zugriff oder ausschließlich ein verschlüsselter (HTTPS) Zugriff erlaubet werden.

Bei aktiver sicheren HTTPS Verbindung kann über folgende Zeile auf den Videoserver zugegriffen werden:
https:\\“IP-Adresse“
Wenn Sie über die HTTPS Verbindung streamen wollen, verwenden Sie folgenden Link:
https:\\“IP-Adresse“:“HTTPS-Port“\Live.sdp

Zertifikate erstellen und installieren

„Selbstsigniertes Zertifikat automatisch erstellen“ Es wird das in dem Videoserver vordefinierte Zertifikat genutzt. Hierbei können keine Einstellungen vom Benutzer vorgenommen werden.

„Selbstsigniertes Zertifikat erstellen“ Es wird ein neues Zertifikat erstellt. Es müssen spezifische Daten eingegeben werden.

„Zertifikatanfrage erstellen und Installieren“ Mit dieser Option kann eine Zertifikatanfrage generiert werden, welche an eine Zertifizierungsstelle eingereicht werden kann. Es kann auch ein durch eine anerkannte Zertifizierungsstelle (z.B.: VeriSign) ausgestelltes Zertifikat auf dem Videoserver installiert werden.

Anmerkung: Verwenden Sie ein „selbstsigniertes Zertifikat“, werden Sie ggf. einen Warnhinweis von Ihrem Browser erhalten. Selbstsignierte Zertifikate werden immer vom Webbrowser als unsicher eingestuft, da weder ein Stammzertifikat noch ein Authentizitätsnachweis einer Zertifizierungsstelle vorliegt.

6.4 SNMP

Das Simple Network Management Protocol ist ein Netzwerkprotokoll, um Netzwerkgeräte (z. B. Router, Server, Switches, Drucker, Computer usw.) von einer zentralen Station aus zu überwachen und steuern zu können. Das Protokoll regelt hierbei die Kommunikation zwischen den überwachten Geräten und der Überwachungsstation. Aktivieren Sie diese Funktion, wenn Sie ein SNMP-Management-Server in Ihrem Netzwerk einsetzen. Sie können auch auf Softwarelösungen zurückgreifen, die auf Ihrem PC-System installiert werden können.

„Aktiveren von SNMPv1, SNMPv2c“ Abhängig von den Einstellungen Ihres SNMP-Servers können Sie hier Namensfelder der Schreib/Lesen Gruppen festlegen

SNMP Konfiguration

☑ Aktivieren SNMPv1, SNMPv2c

SNMPv1, SNMPv2c Einstellungen

Lesen/Schreiben Gruppe: Private

Nur lesen Gruppe: Public

☐ Aktivieren SNMPv3

Speichern

SNMPView 2.5 current values

Program View Options Start Stop Help

location	system	name	uptime
TVIP52500	Mega-Pixel Network Camera	Mega-Pixel Network Camera	0d, 0h, 14m, 3s

„Aktivieren von SNMPv3“ Unterstütz Ihr SNMP-Server das SNMP-Protokoll in der Version3, können Sie die Statusabfragen verschlüsselt durchführen. Hierzu muss für die Abfrage der Schreib/Lesegruppen ein Verschlüsselungsalgorithmus und Passwort in dem Videoserver und SNMP-Server gespeichert werden.

6.5 Netzwerk

6.5.1 Netzwerkeinstellungen

Sämtliche Änderungen, die auf dieser Seite vorgenommen werden, führen zu einem Neustart des Systems, um diese Änderungen wirksam werden zu lassen. Stellen Sie sicher, dass die Felder jeweils richtig ausgefüllt sind, bevor Sie auf „Speichern“ klicken.

„**LAN**“ Die Voreinstellung ist LAN. Verwenden Sie diese Einstellung, wenn der Videoserver mit einem LAN verbunden ist. Dazu sind weitere Einstellungen wie IP-Adresse oder Subnetzmaske nötig.

„IP-Adresse automatisch beziehen“ Bei jedem Neustart des Videoservers wird dieser eine IP-Adresse über einen DHCP-Server zugewiesen.

„**Feste IP-Adresse verwenden**“ Die Netzwerkdaten wie z.B. die IP-Adresse werden hier fest vergeben.

“**IP-Adresse**” Diese wird zur Netzwerk-Identifizierung benötigt.

“**Subnetz-Maske**” Diese dient zur Bestimmung, ob das Ziel sich im selben Subnetz befindet. Der Standardwert lautet “255.255.255.0”.

“**Standard-Router**” Dies ist der Gateway für die Weiterleitung von Bildern an ein anderes Teilnetz. Eine ungültige Router-Einstellung wird die Übertragung an diese Ziele in verschiedenen Teilnetzen verhindern. Besteht eine Cross-Link-Kabel-Verbindung geben Sie bitte hier unbedingt eine IP im gleichen Subnetzbereich des Videoservers ein (z.B. 192.168.0.1).

“**Primäre DNS**” Server der primären Domänenbezeichnung, mit welchem die Host-Namen in IP-Adressen umgewandelt werden.

“**Sekundäre DNS**” Server der sekundären Domänenbezeichnung zur Erstellung einer Reservekopie der primären DNS.

„**UPnP verwenden**“ Das Universal Plug and Play wird hiermit aktiviert. Wenn Ihr Betriebsystem UPnP unterstützt, kann der Videoserver direkt über die UPnP-Verwaltung angesprochen werden (Windows : Netzwerkumgebung)

Stellen Sie sicher, dass die Option „UPnP verwenden“ immer aktiviert ist. UPnP wird auch für das Auffinden des Videoservers von eytron VMS benutzt.

„**UPnP Portweiterleitung AN**“ Die Universal Plug and Play-Portweiterleitung für Netzwerkdienste wird hiermit aktiviert. Unterstütz ihr Router UPnP, wird mit dieser Option automatisch die Portweiterleitung für Video-Streams Router-seitig für den Videoserver aktiviert.

„PPPoE“ Verwenden Sie diese Einstellung wenn der Videoserver direkt mit einem DSL-Modem verbunden ist. Benutzername und Passwort erhalten Sie von Ihrem ISP (Internet Service Provider).

„IPv6“ Verwenden Sie diese Funktion um mit IP-Adressen der Generation v6 zu arbeiten.

☑ Aktivieren IPv6

IPv6 Informationen

☑ IP Adresse manuell einstellen

Optionale IP Adresse / Präfix Länge / 64

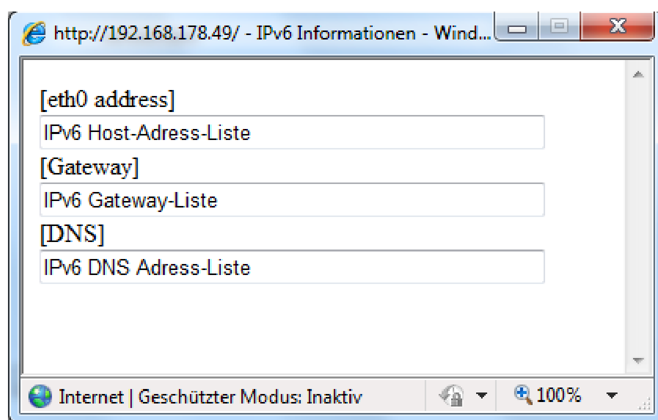
Optionaler Standard Router

Optionale Primäre DNS Adresse

Bitte beachten Sie, dass Ihr Netzwerk und die Hardware IPv6 unterstüzen muss.

Wenn IPv6 aktiviert ist, wartet der Videoserver standardmäßig, bis er vom Router eine IPv6 Adresse mittels DHCP zugewiesen bekommt.
Falls kein DHCP Server vorhanden ist, stellen Sie die IP Adresse manuell ein.
Hierzu „IP Adresse manuell einstellen“ aktivieren und IP Adresse,Standard Router und DNS Adresse eintragen.

“IPv6 Information“ Es werden alle IPv6 Informationen in einem separaten Fenster angezeigt.



Wenn die IPv6 Einstellungen korrekt sind, können Sie alle Einstellungen im unteren Fenster ablesen.

[eth0 address]

2001:0c08:2500:0002:0202:d1ff:fe04:65f4/64@Global

fe80:0000:0000:0000:0202:d1ff:fe04:65f4/64@Link

[Gateway]

fe80::211:d8ff:fea2:1a2b

[DNS]

2010:05c0:978d::

6.5.2 IEEE 802.1x

Aktivieren Sie diese Funktion, wenn Ihre Netzwerkumgebung den Standard IEEE 802.1x, eine Port basierte Zugriffskontrolle im Netzwerk, verwendet.
IEEE 802.1x verbessert die Sicherheit von lokalen Netzwerken.
Eine Verbindung wird nur genehmigt, wenn alle Zertifikate zwischen Server und „Kunde“ verifiziert wurden.
Dies geschieht durch einen Authentifizierer in Form von einem Switch/Access Point welcher Anfragen an den RADIUS Authentifizierungsserver schickt.
Ansonsten wird keine Verbindung hergestellt und der Zugriff auf den Port verweigert.

Bitte beachten Sie, dass Ihre Netzwerkkomponenten so wie der RADIUS Server den Standard IEEE 802.1x unterstützen muss.

6.5.3 HTTP

“**HTTP-Port**” Dies kann ein anderer Port als der vorgegebene Port 80 sein (80, oder 1025 - 65535). Nach dem Ändern des Ports muss der Benutzer über die Änderung informiert werden, um eine erfolgreiche Verbindung zu gewährleisten. Wenn der Administrator beispielsweise den HTTP-Port des Videoservers, dessen IP-Adresse 192.168.0.99 lautet, von 80 auf 8080 abändert, muss der Benutzer anstelle der “http://192.168.0.99” die “http://192.168.0.99:8080” in den Web-Browser eingeben.

„**Sekundärer HTTP-Port**“ Zusätzlicher HTTP-Port für den Videoserverzugriff

Für den direkten Zugriff auf einzelne Video-Streams über Web sind nachfolgende Zugangsnamen einstellbar. Der Zugriff erfolgt über komprimierte JPEG Bilder und ermöglicht Webbrowser (Firefox, Netscape), die kein ActiveX-Plugin verarbeiten können, den direkten Zugriff auf den Video-Stream:

„Zugangsname für Stream 1“ Zugangsname für den MJPEG Stream 1
„Zugangsname für Stream 2“ Zugangsname für den MJPEG Stream 2
„Zugangsname für Stream 3“ Zugangsname für den MJPEG Stream 3
„Zugangsname für Stream 4“ Zugangsname für den MJPEG Stream 4

Anmerkung: Der Internet-Explorer unterstützt keine Darstellung von MJPEG Bildern ohne Active X

6.5.4 FTP

„**FTP-Port**“ Dies ist der interne FTP-Server-Port. Dies kann ein anderer Port als der vorgegebene Port 21 sein (21, oder 1025 - 65535). Über FTP können die auf dem Videoserver gespeicherten Videodaten direkt abgerufen werden. Verwenden Sie hierfür ein eigenständiges FTP-Programm.

Das Adressformat für die Eingabe der Verbindungsdaten ist wie folgt aufgebaut:
Server: IP-Adresse des Videoservers
Benutzername: Administratorbenutzer
Passwort: Passwort des Administrators
Port: FTP-Port des Videoservers

Beispiel (mit FTP-Programm)
Server: 192.168.0.99
Benutzername: root
Passwort: admin
Port: 1026

Server: /mnt/auto/CF/NCMF

- /
  - mnt
    - auto
      - CF
        - NCMF
        - ncmf
    - CF

Dateiname /	Dateigröße	Dateityp	Zuletzt geändert	Berechtigu...	Besitzer/Gr...
000_1283513262.jpg	77.915	JPEG-Bild	03.09.2010 11:2...	-rwxr-xr-x	root root
000_1283513305.jpg	77.966	JPEG-Bild	03.09.2010 11:2...	-rwxr-xr-x	root root
000_1283513366.jpg	77.821	JPEG-Bild	03.09.2010 11:2...	-rwxr-xr-x	root root
000M.jpg	77.098	JPEG-Bild	03.09.2010 11:2...	-rwxr-xr-x	root root
001.jpg	77.218	JPEG-Bild	03.09.2010 11:2...	-rwxr-xr-x	root root
001M.jpg	77.259	JPEG-Bild	03.09.2010 11:2...	-rwxr-xr-x	root root
001M_1283513256.jpg	77.638	JPEG-Bild	03.09.2010 11:2...	-rwxr-xr-x	root root
001M_1283513303.jpg	78.269	JPEG-Bild	03.09.2010 11:2...	-rwxr-xr-x	root root
001M_1283513364.jpg	77.926	JPEG-Bild	03.09.2010 11:2...	-rwxr-xr-x	root root
002.jpg	77.267	JPEG-Bild	03.09.2010 11:2...	-rwxr-xr-x	root root
002_1283513268.jpg	78.236	JPEG-Bild	03.09.2010 11:2...	-rwxr-xr-x	root root
002_1283513310.jpg	78.411	JPEG-Bild	03.09.2010 11:2...	-rwxr-xr-x	root root
002_1283513368.jpg	77.496	JPEG-Bild	03.09.2010 11:2...	-rwxr-xr-x	root root
20100903_112614.mp4	542.681	MPEG-4 M...	03.09.2010 11:2...	-rwxr-xr-x	root root
20100903_112711.mp4	546.532	MPEG-4 M...	03.09.2010 11:2...	-rwxr-xr-x	root root
20100903_112819.mp4	547.002	MPEG-4 M...	03.09.2010 11:2...	-rwxr-xr-x	root root
normal-1283513308_2073467...	35.217.960	3GPP Movie	03.09.2010 11:2...	-rwxr-xr-x	root root
normal-1283513368_1099627...	2.565.197	3GPP Movie	03.09.2010 11:2...	-rwxr-xr-x	root root

19 Dateien und 2 Verzeichnisse. Gesamtgröße: 40.507.467 Bytes

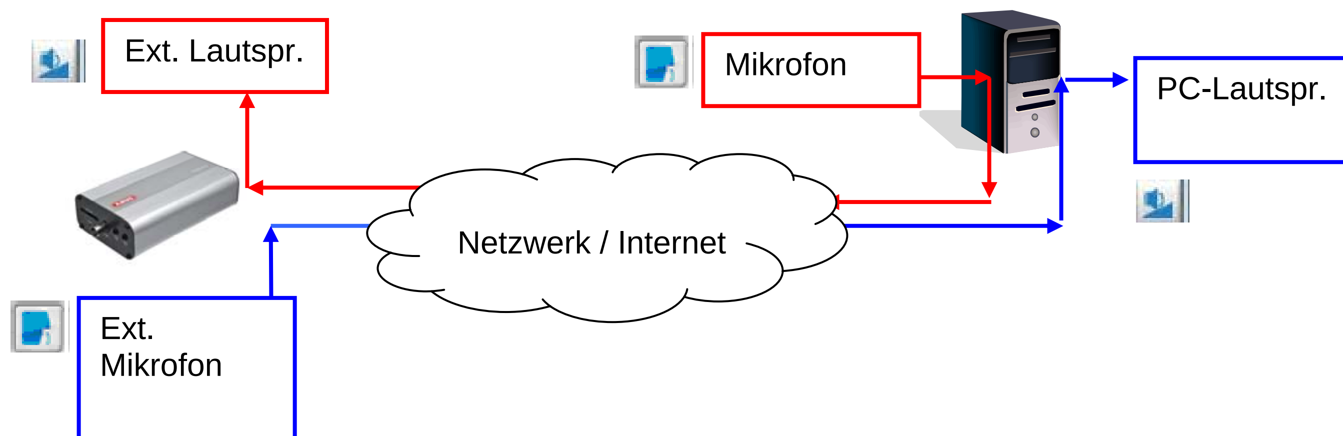
6.5.5 HTTPS

„**HTTPS-Port**“ Dies ist die Porteinstellung für den internen HTTPS-Port. Dies kann ein anderer Port als der vorgegebene Port 443 sein (443 oder 1025 - 65535). Weitere Einstellmöglichkeiten für HTTPS finden Sie unter 5.5.3

6.5.6 Zwei Wege Audio

„Zwei Wege Audio“ Dies ist der Port für die Zwei Wege Audio Funktion. Dies kann ein anderer Port als der vorgegebene Port 5060 sein (5060 oder 1025 - 65535).

Um die Zwei-Wege-Audio Funktion nutzen zu können, müssen Sie unter **„Video und Audio“** für den gewählten Video-Stream MPEG-4/H.264 aktivieren. MJPEG unterstützt ausschließlich die Übertragung von Videodaten und ist deshalb für diese Funktion nicht geeignet.



Live-Stream Funktionen:

Starten Sie die Übertragung der Audiodaten.

Regelt die Empfindlichkeit des Audioeingangs des Videoservers.

Schalten Sie das Mikrofon/Audioeingang aus.

Klicken Sie die Schaltfläche erneut, um die Audioübertragung zu stoppen.

6.5.7 RTSP Übertragung

„**RTSP-Authentifizierung**“ Die Authentifizierung kann disable (Standard) oder Basic (einfach) bzw. erweiterter Modus (digest) sein.

Ist die RTSP-Authentifizierung aktiviert, so muss beim RTSP Verbindungsaufbau ein Benutzername und ein Passwort eines gültigen Benutzers eingegeben werden (z.B. Administrator).
HINWEIS: Die RTSP Authentifizierung muss vom Videoplayer unterstützt werden (z.B. Realplayer 10.5).

„**Zugangsname für Stream 1**“ Dies ist der Zugangsname 1, um eine Verbindung von einem Client herzustellen. Der Codec-Typ muss MPEG4 sein! Verwenden Sie rtsp://<IP-Adresse>:RTSP-port /<Zugangsname 1>, um eine Verbindung herzustellen.

„**Zugangsname für Stream 2**“ Dies ist der Zugangsname 2, um eine Verbindung von einem Client herzustellen. Der Codec-Typ muss MPEG4 sein! Verwenden Sie rtsp://<IP-Adresse>:RTSP-port /<Zugangsname 2>, um eine Verbindung herzustellen.

„**Zugangsname für Stream 3**“ Dies ist der Zugangsname 3, um eine Verbindung von einem Client herzustellen. Der Codec-Typ muss MPEG4 sein! Verwenden Sie rtsp://<IP-Adresse>:RTSP-port /<Zugangsname 3>, um eine Verbindung herzustellen.

„**Zugangsname für Stream 4**“ Dies ist der Zugangsname 4, um eine Verbindung von einem Client herzustellen. Der Codec-Typ muss MPEG4 sein! Verwenden Sie rtsp://<IP-Adresse>:RTSP-port /<Zugangsname 4>, um eine Verbindung herzustellen.

RTSP Zugriff mit VLC:
rtsp://192.168.0.99:10052/live.sdp

„**RTSP-Port**“ Dieser Port kann vom voreingestellten Port 554 abweichen (554; oder 1025 bis 65535). Beachten Sie bei Abänderung das Eingabeformat analog zum HTTP-Port.

„**RTP-Port für Video**“ Dieser Port kann vom voreingestellten Port 5558 abweichen. Die Portnummer muss geradzahlig sein.

„**RTCP-Port für Video**“ Dieser Port muss der „RTP-Port für Video“ plus 1 sein.

„**RTP-Port für Audio**“ Dieser Port kann vom voreingestellten Port 5556 abweichen. Die Portnummer muss geradzahlig sein.

„**RTCP-Port für Audio**“ Dieser Port muss der „RTP-Port für Audio“ plus 1 sein.

6.5.8 Multicast Übertragung

Multicast bezeichnet eine Nachrichtenübertragung von einem Punkt zu einer Gruppe (auch Mehrpunktverbindung genannt). Der Vorteil von Multicast besteht darin, dass gleichzeitig Nachrichten an mehrere Teilnehmer oder an eine geschlossene Teilnehmergruppe übertragen werden können, ohne dass sich beim Sender die Bandbreite mit der Zahl der Empfänger multipliziert. Der Sender braucht beim Multicasting nur die gleiche Bandbreite wie ein einzelner Empfänger. Es findet eine Vervielfältigung der Pakete an jedem Netzwerkverteiler (Switch, Router) statt.

Multicast ermöglicht in IP-Netzwerken effizient Daten an viele Empfänger zur gleichen Zeit zu senden. Das passiert mit einer speziellen Multicast-Adresse. In IPv4 ist hierfür der Adress-Bereich 224.0.0.0 bis 239.255.255.255 reserviert.

Folgende Multicasteinstellungen können für Stream 1 - 4 in dem Videoserver konfiguriert werden.

„**Immer Multicast**“ Aktivieren, um Multicast zu verwenden.

“**Multicast Gruppenadresse**” Spezifiziert eine Gruppe von IP-Hosts die dieser Gruppe angehören

“**Multicast Video Port**” Dieser Port kann vom voreingestellten Port 5560 abweichen. Die Portnummer muss geradzahlig sein.

“**Multicast RTCP Video Port**” Dieser Port muss der „Multicast Video Port“ plus 1 sein.

“**Multicast Audio Port**” Dieser Port kann vom voreingestellten Port 5562 abweichen. Die Portnummer muss geradzahlig sein.

“**Multicast RTCP Audio Port**” Dieser Port muss der „Multicast Audio Port“ plus 1 sein.

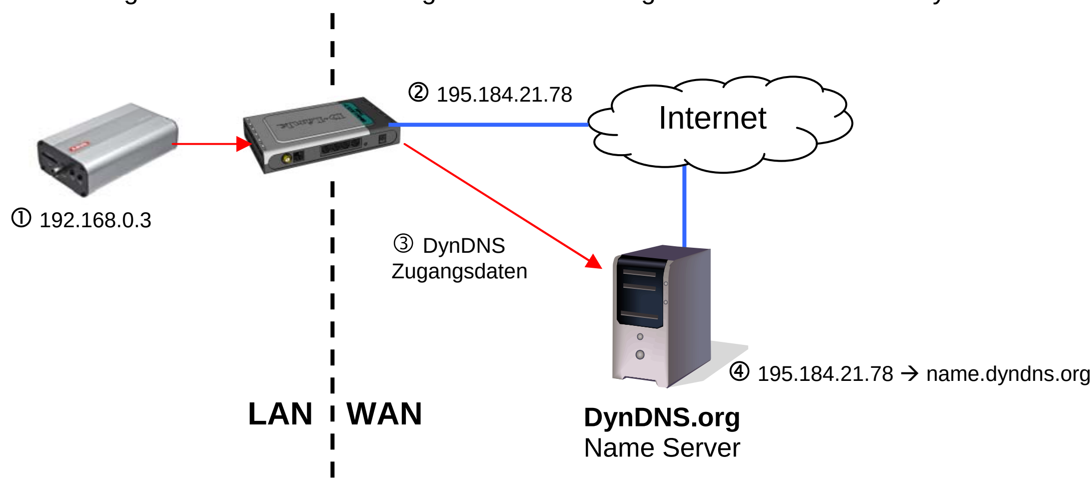
“**Multicast TTL**” Time to Live

Falls Sie eine Portweiterleitung in einem Router einrichten, so sind immer alle Ports weiterzuleiten (RTSP + HTTP). Dies ist für eine erfolgreiche Kommunikation nötig.

7. DDNS

DynDNS oder DDNS (dynamischer Domain-Name-System-Eintrag) ist ein System, das in Echtzeit Domain-Name-Einträge aktualisieren kann. Der Videoserver verfügt über einen integrierten DynDNS-Client, der selbstständig die Aktualisierung der IP-Adresse beim einem DynDNS-Anbieter durchführen kann. Sollte sich der Videoserver hinter einem Router befinden, empfehlen wir die DynDNS-Funktion des Routers zu verwenden.

Die Abbildung veranschaulicht den Zugriff / Aktualisierung der IP-Adresse beim DynDNS-Dienst.



“**DDNS aktivieren**” Mit dieser Option wird die DDNS-Funktion aktiviert.

“**Dienstanbieter**” Die Anbieterliste enthält Hosts, welche die DDNS-Dienstleistungen anbieten. Stellen Sie eine Verbindung mit der Webseite des Dienstleistungsanbieters her, um sicherzustellen, dass die Dienstleistung verfügbar ist.

“**Host-Name**” Zur Anwendung der DDNS-Dienstleistung muss dieses Feld ausgefüllt werden. Geben Sie die Host-Namen ein, der beim DDNS-Server registriert ist.

“**Benutzername/Email**” Der Benutzername und die Email müssen im Feld eingegeben werden, um eine Verbindung mit dem DDNS-Server herzustellen oder um die Benutzer über die neue IP-Adresse zu informieren. Hinweis: Wird in dieses Feld der “Benutzername” eingegeben muss in das folgende Feld das “Passwort” eingegeben werden.

“**Passwort**“ Zur Inanspruchnahme der DDNS-Dienstleistung geben Sie hier Ihr Passwort ein.

DDNS: Dynamic domain name service

DDNS aktivieren:

Anbieter: Dyndns.org(Dynamic)

Hostname:

Benutzername:

Passwort:

Speichern

7.1 DDNS Konto einrichten

Neues Konto bei DynDNS.org einrichten

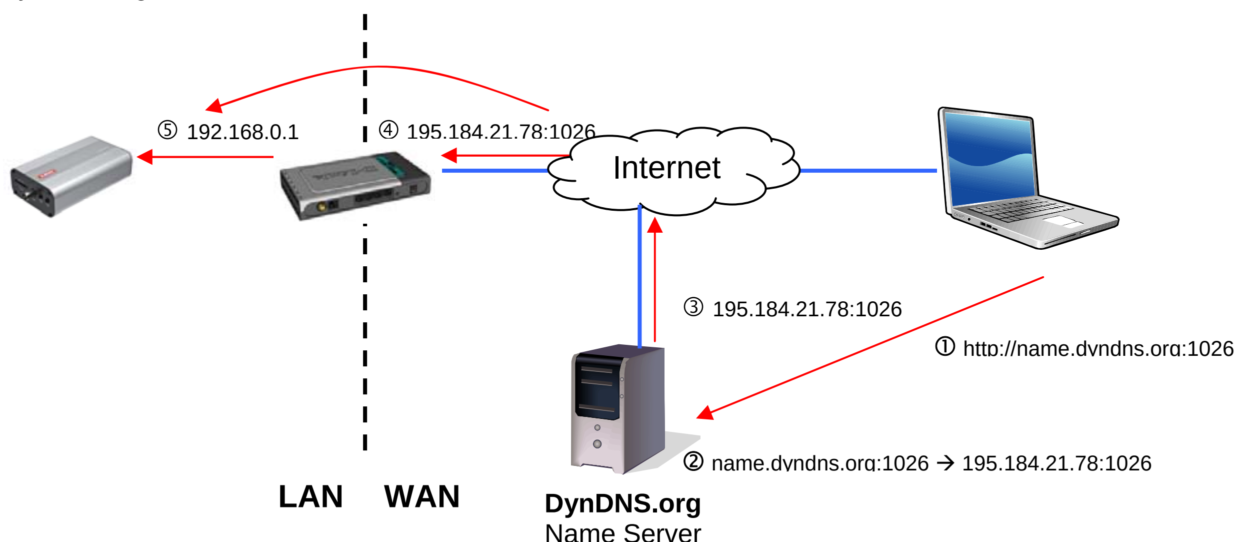
Account Informationen hinterlegen

Notieren Sie Ihre Benutzerdaten und übertragen Sie diese in die Konfiguration des Videoservers

7.2 DDNS Zugriff über Router

Sollte sich Ihr Netzwerkvideoserver hinter einem Router befinden, ist der Zugriff über DynDNS im Router zu konfigurieren. Hierzu finden Sie auf der ABUS Security-Center Homepage www.abus-sc.com eine Beschreibung zur DynDNS-Router-Konfiguration zu gängigen Router-Modellen.

Folgende Abbildung veranschaulicht den Zugriff auf einen Videoserver hinter einem Router über DynDNS.org.



Für den DynDNS Zugriff über einen Router muss eine Portweiterleitung aller relevanten Ports (mindestens RTSP + HTTP) im Router eingerichtet werden.

8. Zugangsliste

Hier steuern Sie die Zugriffe auf den Videoserver anhand von IP-Adresslisten.

“Max. Anzahl gleichzeitiger Verbindungen limitiert auf“ Anzahl der gleichzeitig möglichen Zugriffe auf den Videoserver. Abhängig von der zur Verfügung stehenden Bandbreite des Videoservers, kann es sinnvoll den Zugriff zu beschränken.
„Zugangsliste aktivieren“ Aktiviert die unter „Filter“ definierten IP-Adressfilter

Sie haben zwei Möglichkeiten die IP-Adressfilterung zu definieren.

- Filtertyp „erlauben“: Nur IP-Adressen im definierten Adressraum haben Zugriff
- Filtertyp „verweigern“: IP-Adressen im definierten Adressraum haben keinen Zugriff

Klicken Sie auf „Hinzufügen“ um die Adressbereiche zu konfigurieren. Folgende Einstellmöglichkeiten sind gegeben:

Allgemeine Einstellungen

Max. Anzahl gleichzeitiger Verbindungen limitiert auf: 10 | Informationen anzeigen

Zugangsliste aktivieren

Speichern

Filter Typ

Erlauben | Verweigern

Speichern

Filter

IPv4 Zugangsliste

Hinzufügen | Löschen

Administrator IP Adresse

Zugriff immer zulassen

Speichern

Regel: Einzel, Bereich, Netzwerk:

- Einzel: eine spezifische IP-Adresse wird hinzugefügt
- Bereich: Es können IP-Adressbereiche von – bis definiert werden
- Netzwerk: Es können IP-Adressen mit spezifischer Subnetmaske definiert werden

IPv4 Filter hinzufügen

Adressfilter

Regel: Einzeln

Einzeln
Netzwerk
Bereich

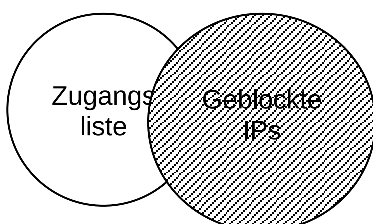
IP Adres

OK | Abbruch

Beispiel:
Der IP-Adressbereich von 192.168.0.1 bis 192.255.255.255 soll zugelassen werden.
Folgende IP-Adressen sollen gesperrt werden 192.168.1.0 bis 192.168.255.255

Ergebnis:
Es dürfen nur Zugriffe von IP's aus folgendem Bereich durchgeführt werden: 192.168.0.1 – 192.168.0.255

Es wird immer eine Schnittmenge zwischen Erlaubten Zugriffen und gesperrten IP's gebildet.



9. Audio und Video

Video-Einstellungen

Videotitel:

Farbe: Farbe

Modulation: Auto

Video-Puffer: Stream 4

Videoausrichtung: Kippen Spiegeln

Titel und Zeitstempel einblenden.

Bildeinstellungen Privatzonenmaskierung

Video Qualitätseinstellungen für Stream 1:

Video Qualitätseinstellungen für Stream 2:

Video Qualitätseinstellungen für Stream 3:

Video Qualitätseinstellungen für Stream 4:

Audio Einstellungen

Stumm

Mikrophoneingang: 0 dB

Audio-Typ:

AAC:

AAC Bit Rate: 16 Kbps

GSM-AMR:

G.711:

Modus: pcmu

Speichern

“**Videotitel**” Der Text erscheint im schwarzen Balken über dem Video-Fenster mit einem Zeitstempel. Dieser Zeitstempel (Datum und Uhrzeit) wird von der integrierten Echtzeituhr des Videoservers geliefert.

“**Farbe**” Wählen Sie zwischen farbiger und schwarz/weißer Darstellung.

„Modulation“ Wählen Sie zwischen dem Videostandart NTSC und PAL oder einer automatischen Erkennung des Videosignals durch den Videoserver.

“Video-Puffer” Der selektierte Video Stream wird für die Aufzeichnung von Vor- und Nachalarm Videodaten (siehe Abschnitt „Anwendung“) genutzt.

“**Kippen”** Zum horizontalen Rotieren des Videos. Wählen Sie diese Optionen aus, falls die Kamera umgekehrt installiert wurde.

“**Spiegeln**” Zum vertikalen Rotieren des Videos.

Verwenden Sie die Option Kippen + Spiegeln, wenn die Kamera an der Decke installiert ist.

„Video Titel und Zeitstempel einblenden“ Mit dieser Option können Titel und Zeitstempel direkt in das Videobild und Momentaufnahmen eingeblendet werden. Die Eingabe unter Punkt „Videotitel“ wird hier verwendet.

9.1 Bildeinstellungen

„Helligkeit, Kontrast, Sättigung, Schärfe“
Passen Sie die Werte entsprechend Ihrer Lichtverhältnisse an.

Sollten Sie die Lichtverhältnisse der Kamera ändern, können die Bildeinstellungen für schlechte Lichtverhältnisse, bei guten Lichtverhältnissen einen negativen Einfluss auf die Bildqualität haben.

Um die geänderten Einstellungen der Bilder anzusehen, klicken Sie auf „Vorschau“. Um die Bildparameter zu übernehmen, klicken Sie auf „Speichern“. Möchten Sie die Änderungen nicht übernehmen, klicken Sie auf „Wiederherstellen“.

9.2 Privatzonenmaskierung

Mit dieser Funktion können Bereiche im Videobild ausgeblendet werden. Es können maximal 5 beliebig große Bereiche markiert werden.

Aktivieren Sie zuerst diese Funktion durch Setzen des Auswahlhakens bei **„Privatzonenmaskierung aktivieren“**.

Über die Schaltfläche **„Neu“** wird ein neues Fenster erstellt, die Größe kann anschließend angepasst werden. Drücken Sie **„Speichern“**, um die Einstellungen zu übernehmen.

Diese Funktion sollte nicht aktiviert werden, wenn die PTZ / ePTZ Funktion der Kameras genutzt wird.
Diese Funktion kann nur konfiguriert werden, wenn als Browser der MS Internet Explorer verwendet wird (ActiveX Modus).

9.3 Grundeinstellung:

Videooptionen
Der Videoserver stellt für den flexiblen Einsatz vier Video Streams in unterschiedlichen Auflösungen zur Verfügung.

- Video Qualitätseinstellungen für Stream 1:
- Video Qualitätseinstellungen für Stream 2:
- Video Qualitätseinstellungen für Stream 3:
- Video Qualitätseinstellungen für Stream 4:

Einstellungen der Streams 1,2,3 und 4
Über das jeweilige Menü konfigurieren Sie Stream 1-4

Die Auflösung bei Stream 4 ist auf QCIF festgelegt. Um auf mobile Geräte zu streamen verwenden Sie Stream 4.

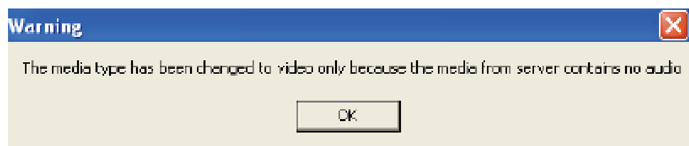
„Bildkompression“ Wählen Sie zwischen H.264/MPEG-4/MJPEG.
„Bildgrösse“ Stellen Sie hier die gewünschte Auflösung ein.
„max.Bildrate“ Stellen Sie hier die maximale Bildwiederholungsrate ein.
„Schlüsselbild-Intervall“ Legt fest wie oft ein I-Frame erzeugt wird. Je kürzer das Intervall, desto bessere Bildqualität wird erreicht, allerdings auf Kosten von höhrerer Netzwerkauslastung.
„Videoqualität Fixe Bildrate“ Legt die Bildrate konstanst auf einen Wert fest. Die Bildqualität sinkt bei Zunahme der Bildkomplexität (z.B.: Bewegung).
„Fixe Bildqualität“ Legt die Bildqualität auf einen konstanten Wert fest. Die Bitrate steigt bei Zunahme der Bildkomplexität (z.B.: Bewegung).

Kompression → / Aufnahmedauer ↓	**H.264**	**MPEG-4**	**MJPEG**
1 Minute Videosequenz in D1 Auflösung mit Qualität „gut“	Ca.**12** MB	Ca.**14** MB	Ca.**60** MB
Speicherkapazität **32 GB** SD Karte	Ca.**43** Stunden	Ca.**36** Stunden	Ca.**9** Stunden

Am Ende des Handbuches finden Sie eine detalierte Tabelle mit jeder Qualitätseinstellung kombiniert mit jeder Auflösung

9.4 Audio Einstellungen

“Stumm” Alle Audiofunktionen in dem Videoserver werden deaktiviert. Es erscheint ein Hinweis beim Zugriff auf den Videoserver



„Externe Mikrofon/Audioinput Verstärkung“ Passen Sie den Wert von +21db bis -33db an

„Audiotyp“ Wählen Sie hier den Audiotyp und die gewünschte Bitrate aus. Ein höherer Wert benötigt mehr Bandbreite:

- **„AAC**“ (Advanced Audio Coding) Spezieller Codec für Audiodatenkompression unter MPEG-4/H.264.
- „**GSM-AMR**“ (Global System for Mobile Communications - Adaptive Multi Rate) Sprachcodec im GSM-Mobilfunknetz.
- **„G.711“** pmca/pmcu (Puls Code Modulation)

10. Bewegungserkennung

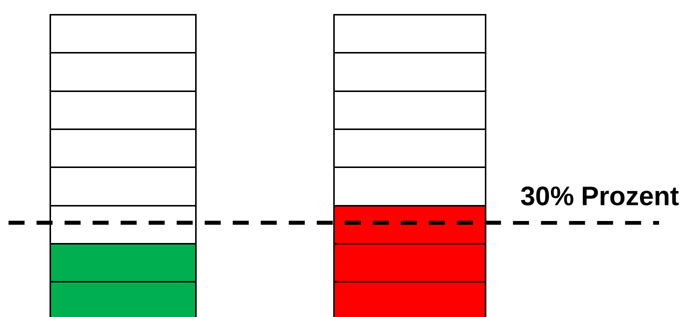
Es können bis zu drei Bewegungszonen in dem Videoserver aktiviert werden. Wählen Sie “**Bewegungsmelder aktivieren**”, um die Konfiguration vorzunehmen.

Die Funktion Bewegungserkennung ist erst nach Festlegen einer Aktion unter dem Menüpunkt „Anwendung“ aktiv.

"**Fenstername**" Der Text erscheint oben im Fenster.
“**Empfindlichkeit**” Empfindlichkeit bei Veränderungen im Bildablauf (Bsp.: Empfindlichkeit hoch: Auslösung bei geringer Bildänderung.
“**Prozent**” Gibt an wie viel Prozent des Bildes sich ändern müssen, damit der Bewegungssensor auslöst.

„Neu“ Klicken Sie auf diese Schaltfläche, um ein neues Fenster hinzuzufügen. Zur Neueinstellung der Größe des Fensters oder zum Verschieben des Titelbalkens klicken Sie mit der linken Maustaste auf den Rahmen des Fensters, halten diesen gedrückt und ziehen ihn mit dem Cursor auf die gewünschte Größe. Durch Anklicken des ‘x’ in der oberen rechten Ecke des Fensters wird das Fenster gelöscht.
„Speichern“ Klicken Sie auf diese Schaltfläche, um die entsprechenden Einstellungen des Fensters zu speichern. Je nach der Bildvariation steigt oder fällt ein Grafikbalken.

Ein grüner Balken bedeutet, dass die Bildvariation sich unterhalb des Überwachungspegels befindet, während ein roter Balken darauf hinweist, dass sich die Bildvariation über dem Überwachungspegel befindet. Wird der Balken rot angezeigt, dann erscheint das erkannte Fenster ebenfalls mit einer roten Umrandung. Beim Zurückgehen auf die Homepage wird das überwachte Fenster ausgeblendet. Der rote Rahmen wird jedoch angezeigt, sobald eine Bewegung erkannt wird.



Grüner Bereich: Bewegung wurde erkannt, führt aber nicht zu einer Alarmauslösung
Roter Bereich: Bildvariation (Bewegung) übersteigt den Grenzwert von 30% und führt zu einem Alarm.

Funktionsweise der Bewegungserkennung:

Sie haben zwei Parameter, um die Bewegungserkennung einzustellen: **Empfindlichkeit** und **Prozent**. Die Abbildung erklärt wie diese beiden Parameter die Bewegungserkennung beeinflussen.

Ausgehend von Abbildung A findet eine Bewegung zu Bild B statt. Die resultierenden Pixeländerungen (in Abhängigkeit der Empfindlichkeitseinstellung) werden in Abbildung C dargestellt (grau). Die Einstellung **„Empfindlichkeit"** bezieht sich auf Fähigkeit der Sensorik Bewegungen im Bild zu erkennen. Desto höher dieser Wert eingestellt ist, desto mehr Pixeländerungen werden im Bild erkannt. Bei einer Bewegungserkennung werden Serverintern die Pixeländerungen (in Abhängigkeit von der Empfindlichkeit) als Alarmpixel gespeichert (Pinke Felder in Abbildung D). Der Schwellwert **„Prozent"** beschreibt hierbei den Anteil der „Alarmpixel" zur Gesamtpixelanzahl im ausgewählten Bereich. Wird der festgelegte Anteil an Alarmpixel (Prozent) erreicht / überschritten wird ein Alarm ausgelöst. Für eine zuverlässige Bewegungserkennung ist es zu empfehlen eine hohe Empfindlichkeit und einen niedrigen Prozentwert einzustellen.

11. Kamera Sabotageerkennung

Der Videoserver unterstützt eine Sabotageerkennung. Ist die Erkennung aktiviert kann ein resultierender Alarm als Ereignis für eine Benachrichtigung genutzt werden (siehe Anwendung)

„Videoserver Sabotageüberwachung aktivieren“ Die Sensorik wird aktiviert.

„Auslöseverhalten“ Der Zeitraum definiert wie lange ein Sabotageereignis vorliegen muss, bis ein Alarm ausgelöst wird.

Folgende Sabotageereignisse werden geprüft:
- Kameraverdrehung
- Kameraabdeckung
- Kameradefokussierung

Diese Sabotageerkennung können Sie als Auslöser in der Kamerafunktion „Anwendung / Ereignis-Setup“ verwenden.

12. Kamerasteuerung

Der Videoserver bietet die Möglichkeit eine analoge PTZ Kamera zu steuern.

RS485 Einstellungen

„Deaktiviert“ RS485-Steuerung ist ausgeschaltet

„PTZ Kamera“ Geben Sie hier die entsprechenden Parameter der PTZ-Kamera ein. Es werden folgende Protokolle unterstützt: Pelco-D, Pelco-P, Samsung scc643, DynaDome/SmartDOME, Lilin PIH-7x00. Sollte ihre PTZ-Kamera keines dieser Protokolle unterstützen wählen Sie bitte „Custom Kamera“

„Transparenter HTTP Tunnel“ Unterstützt Ihr PTZ-Gerät RS485 Kommandos über eine Netzwerkschnittstelle können Sie diese Option wählen. Die notwendigen Parameter müssen Sie der Bedienungsanleitung Ihres PTZ-Gerätes entnehmen.

RS485 Einstellungen

Deaktivieren

PTZ Kamera

Transparenter HTTP Tunnel

Kamera ID: 1

PTZ Treiber: Pelco D protocol

Port-Einstellungen:

Baudrate: 2400

Datenbits: 8

Stopbits: 1

Parität: keine

Voreingestellte Position | Benutzerdefiniertes Kommando

Speichern

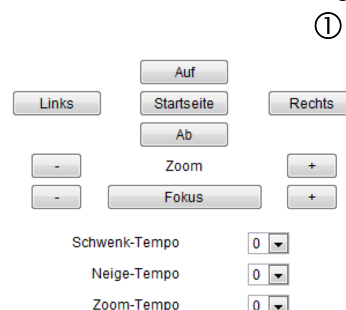
Die genauen PTZ Kommandos entnehmen Sie bitte der Bedienungsanleitung Ihres PTZ Gerätes

„Kamera ID“ Legt die Kamera ID fest.
„PTZ Treiber“ Legt das Protokoll des angeschlossenem PTZ Gerätes fest.
„Baudrate“ Stellen Sie die passende Baudrate ein.
„Datenbits“ Stellen Sie die passenden Datenbits ein.
„Stopbits“ Stellen Sie die passenden Stopbits ein.
„Parität“ Legt die Parität fest.

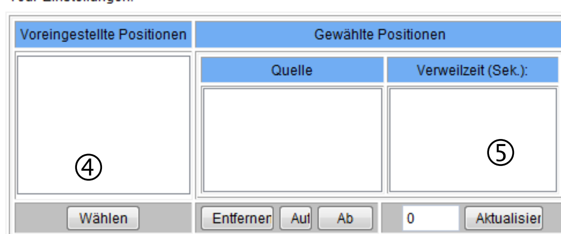
Preset Positionen und Tour einrichten

Es können insgesamt 20 Preset-Positionen im Videoserver gespeichert werden. Gehen Sie hierzu wie folgt vor:

1. Positionieren Sie das Kamerabild über die Richtungstasten auf die gewünschte Einstellung
2. Geben Sie der aktuellen Position einen Preset-Namen und klicken Sie auf hinzufügen. Der Name erscheint in der Preset-Liste
3. Wiederholen Sie die Schritte 1-2 für weitere Presets
4. Markieren Sie die Presets die Sie für eine Tour benutzen wollen und bestätigen Sie diese mit „Wählen“
5. Passen Sie die Verweildauer des jeweiligen Presets falls notwendig an.
6. Speichern Sie die Einstellungen



Tour-Einstellungen:



Speichern

Schliessen

Um die Tour zu starten, drücken Sie „PATROL“ im Livebild des Videoservers. Um diese zu stoppen „STOP“

Benutzerdefiniertes Kommando

Der Menüpunkt „Benutzerderfiniertes Kommando“ ermöglicht Ihnen den direkten Zugriff auf einzelne Funktionen ihres PTZ-Gerätes oder PTZ-Kamera.
In der Regel wird die Funktion dazu verwendet gespeicherte Preset-Positionen oder vordefinierte Touren abzurufen.

Benutzerdefiniertes Kommando

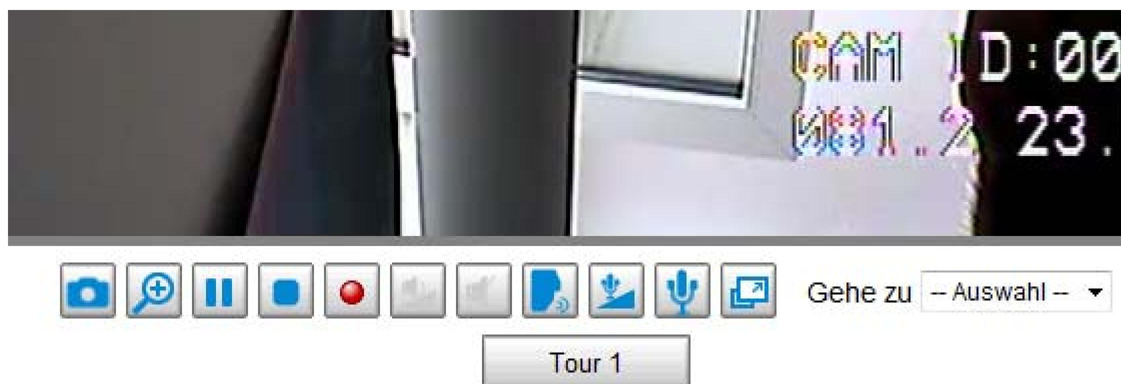
Benutzerdefiniertes Kommando

Wenn Sie "Schaltflächenname" leer lassen, dann wird die Schaltfläche auf der Homepage nicht angezeigt.

	Schaltflächenname	Kommando
Kommando 1:	Tour 1	FF01000900010B
Kommando 2:		
Kommando 3:		
Kommando 4:		
Kommando 5:		

Speichern Schliessen

Mithilfe dieser Funktion können Sie eigene Kommandoschaltflächen im Livebild des Videoservers zur Bedienung/Einstellung des angeschlossenen PTZ-Gerätes erstellen.
Die jeweilige Funktion der Schaltfläche wird durch einen Hexadezimalcode (abhängig vom jeweiligen PTZ-Protokoll) beschrieben.
Alle ABUS Speeddome-Kameras verwenden die Protokolle PELCO D/P.
Es können maximal 5 benutzerdefinierte Schaltflächen erstellt werden.
Unter „Schaltflächenname“ tragen Sie den gewünschten Namen der Schaltfläche ein (z.B.: Tour 1).



Wenn Sie als Kameraprotokoll „Custom Camera“ eingegeben haben,müssen Sie unter „Benutzerdefinitiertes Kommando“ grundlegende Funktionen wie „hoch“,“runter“,“links“,“rechts“ festlegen. Die hierfür zuständigen Codes entnehmen Sie der Anleitung des PTZ-Gerätes.

Wird kein Schaltflächenname angegeben, erscheint die Schaltfläche nicht im Livebild

Das Pelco D/P Protokoll arbeitet aussschliesslich mit Hexadezimalen Zahlen.

Tragen Sie unter „Kommando“ den HEX-Code der gewünschten Funktion ein.
(z.B.: FF 01 00 09 00 01 0B**)**

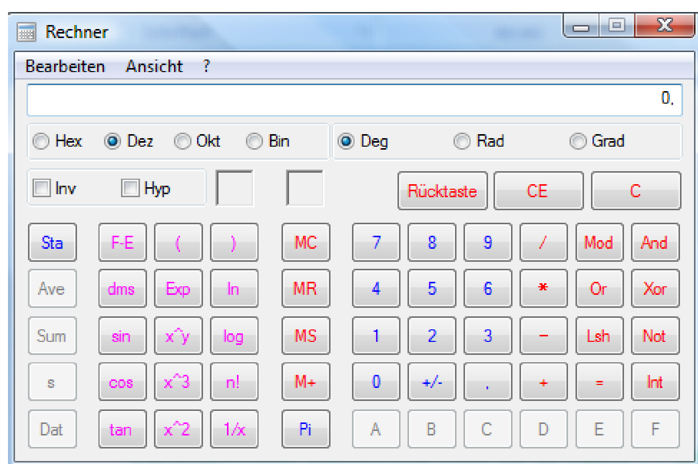
Der Code darf keine Leer-und Sonderzeichen enthalten.
FF 01 00 09 00 01 0B → FF01000900010B

Vorwort Hexadezimal Zahlen
Im folgenden Kapitel wird anhand einiger Beispiele das Hexadezimale Zahlensystem erläutert.

Decimal	Hex	Decimal	Hex	Decimal	Hex
1	1	11	B	30	1E
2	2	12	C	40	28
3	3	13	D	50	32
4	4	14	E	60	3C
5	5	15	F	70	46
6	6	16	10	80	50
7	7	17	11	90	5A
8	8	18	12	100	64
9	9	19	13	500	1F4
10	A	20	14	1000	3E8

Das Hexadezimale Zahlensystem basiert auf Zahlen von 0-9 und Buchstaben von A-F. Bei der Berechnung von Checksummen ist zu berücksichtigen, dass Hexadezimal addiert wird.

Eine wichtige Hilfe zur Umrechnung von Dezimal in Hexadezimal und Addition von Hexadezimal bietet hierfür der in Microsoft Windows integrierte Taschenrechner, welcher hierfür auf „Wissenschaftlich“ eingestellt sein muss.



Dome-Steuerkommandos für TV7600,TV6702,TV7604 (Pelco)

Kommandoszusammensetzung

Wort 1	Wort 2	Wort 3	Wort 4	Wort 5	Wort 6	Wort 7
Synch Byte (immer FF)	Address (ID der analogen Kamera)	Command 1	Command 2	Data 1	Data 2	Check Sum Wort 2-6

Berechnung Check-Summe:

Wort 7= Wort 2 + Wort 3 + Wort 4 + Wort 5 + Wort 6

Worterklärung:

„Wort1“ Immer als „FF“ deklariert
„Wort2“ Bestimmt die ID der analogen Kamera
„Wort3“-„Wort4“ Legt die verschiedenen PTZ Funktionen fest („speichere Preset“, starte Tour“ usw.)
„Wort5“-„Wort6“ Legt zum Beispiel die Numerierung der Presets und Touren fest.
Wenn Sie ein Preset anfahren wollen, muss auch festgelegt werden, welche Presetnummer angefahren werden soll.
„Wort7“ Ist die Summe von Wort 2 – Wort 6 und ist auch als Check Summe bekannt

Beispiel: “Gehe zu Preset 1“ hat den Befehl : FF 01 00 07 00 **01** 09

Wort 1 ist immer auf FF festgelegt
Wort 2 ist immer die ID des Speed Domes
Wort 3 und Wort 4 bestimmen die Funktion: „Zu Preset gehen“
Wort 5 und Wort 6 bestimmt welches Preset angefahren werden soll.
Wort 7 Checksumme

Erläuterung: Im Wort 6 steht die HexZahl 01 für Preset 1.
Würde man nun Preset 15 anfahren wollen, müsste man 0F in das Wort 6 schreiben.

Beispiel: “Gehe zu Preset 15“ hat den Befehl : FF 01 00 07 00 **0F** 17
Diese Vorgehensweisse ist analog bei der Auswahl von Touren oder sonstigen zählbaren Funktionsstrukturen.

Vergessen Sie nicht die Checksumme nach jeder Änderung des Komandos neu zu berechnen.
Eine Änderung des Komandos im obigen Beispiel von Preset 1 zu Preset 15 hätte zur Folge, dass die Checksumme um 14 größer wird!

Befehlsübersicht :

Kommando	Wort 3	Wort 4	Wort 5	Wort 6
Ab	00	10	00	2A
Auf	00	08	00	3C
Links drehen	00	04	2E	00
Rechts drehen	00	02	06	00
Stoppen	00	00	00	00
Menü	00	11	00	00
Tour starten	00	00	09	01 to 08
Scan	00	0F	00	01
Zoom tele	00	20	00	01
Zoom wide	00	40	00	01
Focus near	01	00	00	01
Focus far	00	80	00	00
Iris close	04	00	00	00
Iris open	02	00	00	00
Speichere Preset	00	03	00	01 to C8
Lösche Preset	00	05	00	01 to C8
Gehe zu Preset	00	07	00	01 to C8
Set Auxiliary	00	09	00	01 to 08
Clear Auxiliary	00	0B	00	01 to 08
Remote Reset	00	0F	00	00
Set Zone Start	00	11	00	01 to 08
Set Zone End	00	13	00	01 to 08
Write Char. To Screen	00	15	X Position 00 to 28	ASCII Value
Clear Screen	00	17	00	00
Alarm Acknowledge	00	19	00	Alarm No.
Zone Scan An	00	1B	00	00
Zone Scan Aus	00	1D	00	00
Musterstart setzen	00	1F	00	00
Musterstop setzten	00	21	00	00
Muster abfahren	00	23	00	00
Stelle Zoomspeed ein	00	25	00	00 to 03
Stelle Focus Speed ein	00	27	00	00 to 03
Werkseinstellung der Kamera	00	29	00	00
Auto-Fokus auto/an/aus	00	2B	00	00-02
Auto Iris auto/an/aus	00	2D	00	00-02
AGC auto/an/aus	00	2F	00	00-02
BLC an/aus	00	31	00	01-02
Auto.Weißabgleich an/aus	00	33	00	01-02

13. Anwendung

Hier können Sie Aufgaben in dem Videoserver automatisieren. Die Anwendungskonfiguration besteht aus 3 Bereichen: Ereignis, Server und Medium. Eine typisches Anwendungsbeispiel kann wie folgt aussehen: Aufgrund einer Bewegungserkennung (Ereignis) wird eine E-Mail (Server) zu einem Benutzer mit einem Alarmbild (Medium) versendet.

Ereignis Setup
Klicken Sie auf **„hinzufügen“** um ein neues Ereignis zu erstellen. Es können maximal 3 Ereignisse eingestellt werden.

„Ereignisname“ Vergeben Sie einen eindeutigen Namen unter dem Sie die Ereigniskonfiguration speichern
„Ereignis aktivieren“ Setzen Sie Option, um das programmierte Ereignis zu aktiveren.
„Priorität“ Ereignisse mit höherer Priorität werden zuerst abgearbeitet
„Verzögerung“ Pausenzeit zwischen ausgeführten Ereignissen (z.B.: bei Bewegungserkennung)

Ereignis Setup

Ereignisname:
Ereignis aktivieren
Priorität: Normal
Verzögerung für 10 Sekunde(n).
Hinweis: Dies kann nur für Bewegungssensor und digitalen Eingang angewendet werden.

Auslöser
- Videobewegungssensor
- Periodisch
- Digitaler Eingang
- System Neustart
- Aufzeichnungsalarm
- Kamera-Sabotageüberwachung
- Videoverlust-Alarm
- IP geändert
- Video restore

Ereignis-Zeitplan
Son Mon Die Mit Don Fre Sam
Zeit
- Immer
- Von 00:00 an 24:00 [hh:mm]

Aktion
Digitaler Ausgang aktiv für 1 Sekunden
Videodaten bei Netzwerkausfall sichern
Gehe zu Position: 1
Hinweis: Bitte konfiguriere Voreingestellte Positionen zuerst

Server hinzufügen | Medium hinzufügen

	Server	Medium	
	SD	-----None-----	SD-Karten Test · Anzeigen
	NAS	1	Ordner automatisch erstellen; Angepasster Ordner %Y%M%D/%H; Anzeigen

Speichern | Schliessen

13.1 Auslöser Einstellungen

„Videobewegungssensor“ Aktiveren Sie das gewünschte Bewegungsfenster
„Intervall“ Das Ereignis wird periodisch ausgelöst. Maximale Einstellung ist 999 Minuten
„Digitaler Eingang“ Liegt ein Signal am Alarmeingang an (z.B.: Türkontakt) wird ausgelöst
„System Neustart“ Ereignis wird beim Neustart des Videoservers ausgelöst (vorhergehender Spannungsverlust)
„Aufzeichnungsalarm“ Ist der Zielspeicher (Medium) voll oder wird ein Ringspeicher überschrieben wird ein Alarm ausgelöst.
„Kamera Sabotageüberwachung“ Ein Alarm wird ausgelöst, wenn eine Kamerasabotage der angeschlossenen analogen Kamera erkannt wird.
„**Videoverlust-Alarm“** Ein Alarm wird ausgelöst, wenn das Videosignal ausgefallen ist.
„IP geändert“ Sobald dem Videoserver eine neue IP Adresse zugewiesen wird, wird ein Alarm ausgelöst.
„Videosignal wiederhergestellt“ Liegt das Videosignal nach einer Störung wieder an wird ausgelöst.

Ereignis-Zeitplan

“**Son**” - “**Sam**” wählt die Wochentage zur Ausführung eines Ereignisses.
„**Immer**“ Aktiviert das Ereignis zu jeder Zeit (24 Stunden)
„**Von**“ - „**bis**“ Das Ereignis ist zeitlich eingegrenzt.

13.2 Serverkonfiguration

Es können 5 Server in der Netzwerkkamera gespeichert werden. Klicken Sie auf **„hinzufügen“** um einen neuen Server zu konfigurieren. Der Server vom Typ **„SD“** ist voreingestellt und bezeichnet die SD-Karten-Einheit als Ziel für Datenspeicherungen. Folgende Server-Typen können konfiguriert werden:

- E-Mail: tragen Sie hier die Zugangsdaten ein
- FTP: tragen Sie hier die Zugangsdaten ein. Adresskonvention: ftp.abus-sc.com
- HTTP: tragen Sie hier die Zugangsdaten ein. Adresskonvention: http://abus-sc.com/cgi-bin/upload.cgi
- Netzwerkordner: Adresskonvention: \\192.160.0.5\NAS

Server Name:

Server Typ

(•) E-mail:

Absender E-Mail Adresse:
Empfänger E-Mail Adresse:
Server Adresse:
Benutzername:
Passwort:
Server Port 25
[ ] Dieser Server benötigt eine sichere Verbindung (SSL)

( ) FTP:
( ) HTTP:
( ) Netzlaufwerk:

Test | Speichern | Schliessen

Nach Eingabe der Zugangsdaten müssen die Einstellungen gespeichert werden. Bevor Sie das Fenster schließen, ist es zu empfehlen einen **„Test“** durchzuführen. In einem neuen Fenster des Browsers wird das Ergebnis angezeigt.

13.3 Medien Einstellungen

Es können 5 Medieneinstellungen in dem Viedoserver gespeichert werden.

Medienname:

Medientyp

Momentaufnahme

Quelle: Stream1

Senden 1 Voralarmbild(er) [0~7]

Senden 1 Nachalarmbild(er) [0~7]

Dateiname-Zusatz:

Datum und Uhrzeit an Dateinamen anhängen

Video Clip

Logdatei

Custom Message

Speichern Schliessen

„**Medienname**“ Eindeutiger Name für das Medium.

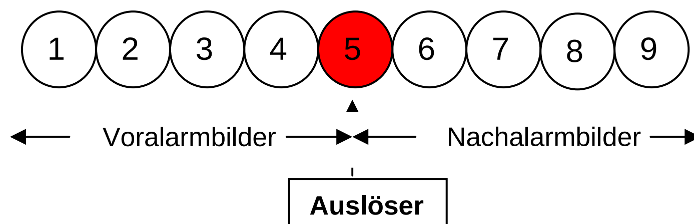
Es existieren 4 verschiedene Medien-Typen:

- Momentaufnahme (Dateiformat JPEG)
- Video Clip (Dateiformat MP4)
- Logdatei (Dateiformat TXT)
- Benutzerdefinierte Mitteilung (Dateiformat TXT)

Jedes angelegte Medium darf nur mit einem Ereignis verknüpft werden.
Eine Doppelbelegung eines Mediums hat eine inkorrekte Arbeitsweise des Videoservers zufolge.
Möchten Sie für zwei Ereignise denselben Medientyp verwenden, müssen zuvor auch zwei separate Medientypen angelegt worden sein.

Momentaufnahme

„**Quelle**“ Die Aufnahme kann von Video-Stream 1-4 erfolgen
„**Sende Voralarmbilder**“ Anzahl der Momentaufnahmen vor einem Ereignis
„**Sende Nachalarmbilder**“ Anzahl der Momentaufnahmen nach einem Ereignis



„**Dateiname-Zusatz**“ Geben Sie hier eine Bezeichnung ein, die dem Dateinamen für die Momentaufnahme vorangestellt wird.
„**Datum und Uhrzeit an Dateiname anhängen**“ Mit dieser Option wird die aufgenommene Momentaufnahme mit dem Datum und der Uhrzeit versehen, um die Dateinamen der Momentaufnahmen entweder im sequentiellen oder ereignisgesteuerten Betrieb leicht voneinander unterscheiden zu können. Beispielsweise bedeutet “video@20030102_030405.jpg”, dass das JPEG-Bild am 2. Januar 2003 um 3 Uhr, 4 Minuten und 5

Sekunden aufgenommen wurde. Wird dieses Suffix ausgelassen, dann wird die Datei mit der Bezeichnung “video.jpg” beim externen FTP-Server nach dem angegebenen Zeitintervall aktualisiert.

Der Dateiname ist wie folgt aufgebaut:
Zusatz_YYYYMMDD_HHMMSS : ABUS_20091115_164501

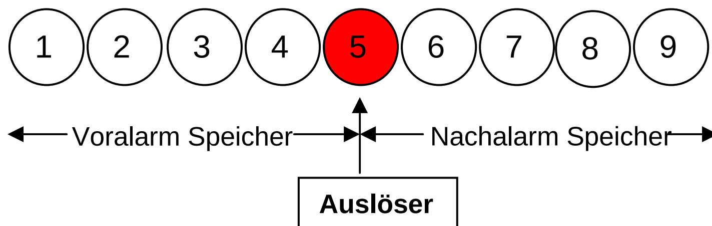
- Zusatz: siehe Dateiname-Zusatz
- Y: Platzhalter für Jahr, YYYY = 2009
- M: Platzhalter für Monat, MM = 11
- D: Platzhalter für Tag, DD = 15
- H: Platzhalter für Stunde, HH = 16
- M: Platzhalter für Minute, MM = 45
- S: Platzhalter für Sekunde, SS = 01

Videoclip

„**Quelle**“ Die Aufnahme kann von Video Stream 1-4 erfolgen.

Es wird der Video Stream als Quelle angeboten, der unter „Audio und Video“ für „Video Puffer“ konfiguriert ist.

„Voralarm-Aufzeichnung“ Voralarm Aufzeichnungsintervall in Sekunden (max. 9 Sekunden)
„Maximale Dauer“ Maximale Dauer pro Datei (max. 10 Sekunden)



„Maximale Dateigröße“ Maximale Größe der Datei in kByte (max. 800 kByte)
„**Dateiname-Zusatz**“ Geben Sie hier eine Bezeichnung ein, die dem Dateinamen für die Videoaufnahme vorangestellt wird (Details siehe Momentaufnahme)

Logdatei
Speichert den aktuellen System-Log-Inhalt in eine Textdatei.

Custom Message
Eine benutzerdefinierte Meldung in Form von einer Textdatei wird mitgesendet.

13.4 Aktion

Aktion

☐ Digitaler Ausgang aktiv für 1 Sekunden

☐ Videodaten bei Netzwerkausfall sichern

☐ Gehe zu Position: 1

Hinweis: Bitte konfiguriere Voreingestellte Positionen zuerst

Server hinzufügen | Medium hinzufügen

	Server	Medium	
☐	SD	-----None-----	SD-Karten Test / Anzeigen
☑	NAS	1	☑ Ordner automatisch erstellen
			Angepasster Ordner %Y%M%D/%H
			Anzeigen

Speichern | Schliessen

Konfigurieren Sie hier die Aktion, welche durchgeführt werden soll, wenn ein ausgelöster Alarm anliegt.
„Digitaler Ausgang aktiv für“ Bei Aktivierung wird der Relaisausgang des Videoservers geschaltet.
„Gehe zu Position“ es wird eine Preset-Position bei Alarm angesteuert
„**Server**“ Zu einem bestimmten Server wird das selektierte Medium gesendet (z.B.: eine Email wird mit einer Momentaufnahme gesendet).

„Ordner automatisch erstellen“ Erstellt automatisch Ordner im Verzeichniss des Netzwerklaufwerkes
„Angepasster Ordner“ Mithilfe von Variablen wird die spezifische Benennung des Ordners festgelegt. Entnehmen Sie die zur Verfügung stehenden Variablen der untenstehenden Tabelle.

Symbol	Beispiel/Funktion
/	*Neuen Unterordner anlegen*
%IP = IP-Adresse	*192.168.0.1*
%N = Eventname	*Motion_W1*
%Y = Jahr	*2010*
%M = Monat	*03*
%D = Tag	*04*
%H = Stunde	*14*
“Beispieltext“	*“Beispieltext”*

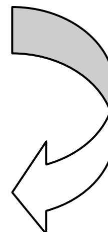
Beispiel:
Folgende Eingabe würde diesen Pfad erstellen.

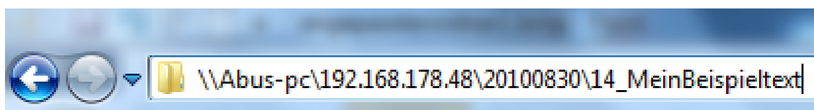
☑ Ordner automatisch erstellen

Angepasster Ordner

%IP/%Y%M%D/%H_MeinBeispieltext

Anzeigen





13.5 Anwendungsübersicht

Hier sehen Sie alle im Videoserver eingerichteten „Ereignisse“, „Medientypen“, und „Server“.
Sie können hier die verschiedenen Einstellungen kontrollieren, löschen und neue hinzufügen.

Ausserdem können verschiedene Parameter wie z.B.
Name, Status, Auslöser, Standort, Adresse kontrolliert werden.

Ereignis Setup

Name	Status	Son	Mon	Die	Mit	Don	Fre	Sam	Zeit	Auslöser
Motiondetection	OFF	V	V	V	V	V	V	V	00:00~24:00	boot

Hinzufügen | Motiondetection | Löschen | Hilfe

Server Einstellungen

Name	Typ	Adresse/Standort
E-mailserver	email	asd
NAS	ns	\\my_nas\disk\folder

Hinzufügen | E-mailserver | Löschen

Medium

Freier Speicherplatz: 9550KB

Name	Typ
Snapshot	snapshot

Hinzufügen | Snapshot | Löschen

14. Aufnahme

Der Bereich Aufnahme dient dazu, Aufnahmen einzurichten mit dem Unterschied, dass hier Permanentvideoaufnahmen für SD-Karte oder Netzwerkfreigaben eingerichtet werden können. Zwei Aufnahmeeinstellungen können im Videoserver gespeichert werden. Erstellen Sie eine neue Aufnahme durch Klick auf **„Hinzufügen“**

Aufnahme-Eintrag-Name:

Aufnahme aktivieren

Priorität: Normal

Quelle: Stream1

Auslöser

Zeitplan

Network fail

Aufnahme-Zeitplan

Son Mon Die Mit Don Fre Sam

Zeit

Immer

Von 00:00 an 24:00 [hh:mm]

Ziel SD

Hinweis: Um den Aufzeichnungsalarm zu aktvieren, konfigurieren Sie bitte Anwendung zuerst

Speichern | Schliessen

Ziel: **„Netzwerklaufwerk“**

Kapazität:

( ) Gesamter freier Speicherplatz

(•) Reservierter Platz: 15 Mbytes

Dateiname-Zusatz:

[ ] Ordner automatisch erstellen

Angepasster Ordner : %Y%M%D/%H

[ ] Ringspeicheraufnahme aktvieren

Hinweis: Um den Aufzeichnungsalarm zu aktvieren, konfigurieren Sie bitte Anwendung zuerst

Speichern | Schliessen

„**Aufnahme Name**“ Ein eindeutiger Name für einen Aufnahmeeintrag.
„**Aufnahme aktivieren**“ Auswahlhaken setzen, um Aufnahmeeintrag zu aktivieren.
„**Priorität**“ Die Aufnahme mit höherer Priorität wird bevorzugt ausgeführt.
„**Quelle**“ Die Aufnahme kann von Video-Stream 1-4 erfolgen.
„Zeitplan“ der Aufnahme Zeitplan wird genutzt
„Netzwerkfehler“ Tritt ein Netzwerkfehler auf, wird die Datenspeicherung automatisch auf SD-Karte aktiviert
“**Son**” - “**Sam**” wählt die Wochentage zur Ausführung der Aufnahme.
„**Immer**“ Aktiviert die Aufnahme zu jeder Zeit.
„**Von**“ - „**bis**“ Die Aufnahme ist zeitlich eingegrenzt.
„**Ziel**“ SD-Karte oder Netzwerkordner
„**Gesamter Speicherplatz**“ Der maximal auf dem Zielspeicher zur Verfügung stehender Speicherplatz wird genutzt.
„**Reservierter Platz**“ Gibt an, wieviel MB freier Speicherplatz vorreserviert werden.

Für genauere Hinweise zu „Ordner automatisch erstellen“ bitte zu Kapitel „13.4 Aktion“ wechseln.

Bei aktivierter Funktion „Angepasster Ordner“ kann die Ringspeicherfunktion nicht verwendet werden.

„Aktiviere Ringspeicher“ Schaltet die Ringspeicherfunktion ein. Wird bei der Datenspeicherung der eingestellte Wert erreicht, werden die ältesten Daten überschrieben.

Aufnahmeübersicht

„Name (Video)“ öffnet die Aufnahmekonfigurationsseite
„Status (ON)“ Setzt den Status der Aufnahme auf AN/AUS
„Ziel (SD)“ Öffnet eine Dateiliste mit den gespeicherten Aufnahmen

Name	Status	Son	Mon	Die	Mit	Don	Fre	Sam	Zeit	Quelle	Ziel
Video	ON	V	V	V	V	V	V	V	00:00~24:00	stream1	SD

Hinzufügen | SD-Karten Test | Video ▾ | Löschen

15. Lokaler Speicher

Dieser Abschnitt erklärt, wie der lokale Speicher (SD-Karte) des Videoservers verwaltet werden kann. Es werden Karten vom Typ SD/SDHC Class 6 von bis zu 32GByte unterstützt.

Verwaltung der SD-Karte

SD-Karten Management

SD-Karten Status: Bereit

Gesamtgröße:	1925464 KBytes	Freie Größe:	1569292 KBytes
Belegter Speicher:	356172 KBytes	Verwenden (%):	18.50 %

Formatieren

SD-Karten Optionen:

- Überschreiben aktivieren
- Automatisches Löschen aktivieren

Max. Dauer für Dateierhalt: 7 Tage

Speichern

Nutzen Sie die **„Format“**-Funktion, wenn Sie die Karte erstmalig in den Videoserver einsetzen

Schalten Sie die Option **„Überschreiben aktivieren“** ein, werden die ältesten Daten zuerst überschrieben, wenn die Speicherkapazität der SD-Karte erreicht ist.

Aktivieren Sie die Option **„Automatisches Löschen“** wird nach Eingabe der maximalen Vorhaltezeit die SD-Karte komplett gelöscht.

Suche und Anzeige der Aufnahmen
Wird kein Kriterium ausgewählt, werden immer alle Aufzeichnungen in der Ergebnisliste angezeigt

Suche und Anzeige der Aufnahmen

Dateiattribute:

Auslöser-Typ:	Digitaler Eingang	Videoverlust	Video restore
	System Neustart	Aufzeichnungsalarm	Bewegungserkennung
	Interval	Netzwerkfehler	IP geändert
	Sabotage		
Medientyp:	Video Clip	Momentaufnahme	Text
Gesperrt:	Gesperrt	Entsperrt	

Trigger time:

Von:	Datum		Zeit	
an:	Datum		Zeit	
		(yyyy-mm-dd)		(hh:mm:ss)

Suche

„Auslöser-Typ“ wählen Sie ein oder mehrere Kriterien aus, anhand der eine Aufzeichnung auf die SD-Karte erfolgte.
„Auslöse-Zeit“ Wählen Sie den gewünschten Zeitraum

Klicken Sie auf „Suche“. Alle den Kriterien zutreffenden Aufzeichnungen werden in der Ergebnisliste angezeigt.

Ergebnisliste

Anzahl der Elemente auf einer Seite

Suchergebnisse

Show 10 entries Search: — Suche

	Trigger time	Medientyp	Auslöser-Typ	Gesperrt
☐	2009-10-12 00:39:50	videoclip	seq	Nein
☐	2009-10-12 00:40:50	videoclip	seq	Nein
☐	2009-10-12 00:41:50	videoclip	seq	Nein
☐	2009-10-12 00:42:50	videoclip	seq	Nein
☐	2009-10-12 00:43:50	videoclip	seq	Nein
☐	2009-10-12 00:44:51	videoclip	seq	Nein
☐	2009-10-12 00:45:51	videoclip	seq	Nein
☐	2009-10-12 00:46:50	videoclip	seq	Nein
☐	2009-10-12 00:47:50	videoclip	seq	Nein
☐	2009-10-12 00:48:50	videoclip	seq	Nein

Showing 1 to 10 of 11 entries — Seiten umblättern

Anzeigen | Download | Gesamte Auswahl entfernen | JPEGs nach AVI | Sperren/Entsprerren | Entfernen

„Anzeigen“ Zeigt die ausgewählte Aufzeichnung in einem neuen Fenster an.
„Download“ Bietet die ausgewählte Aufzeichnung zum Download an.
„JPEG zu AVI“ Mehrere JPEG Einzelbild Aufnahmen können selektiert werden (Auswahl-Box) und werden in eine AVI-Datei umgewandelt.
„Sperren / Entsperren“ Einzelne Aufzeichnungen werden gesperrt. Gesperrte Aufzeichnungen werden nicht durch die zyklische Speicherung überschrieben. Entsperren entfernt dieses Attribut wieder.
„Entfernen“ Gewählte Aufzeichnung wird gelöscht

Sie können alternativ auch die auf der SD-Karte gespeicherten Daten über Ihren SD-Kartenleser an Ihrem PC-System auswerten. Es werden die aufgezeichneten Daten entsprechend Ihrer Dateiendung mit Datum und Uhrzeit im Dateinamen angezeigt.

16. Logdatei

Klicken Sie auf diesem Link auf der Konfigurationsseite, um die Systemprotokolldatei anzuzeigen. Der Inhalt der Datei liefert nützliche Informationen über die Konfiguration und die Verbindung nach dem Starten des Systems. Der Standard der Log-Datei ist RFC 3164. Sie können ebenfalls Daten an einen Log-Server senden. Aktivieren sie dazu die Option „Remote Protokoll“, und geben Sie die IP-Adresse und die Portnummer des Servers ein.

17. Parameterliste

Klicken Sie auf diese Link auf der Konfigurationsseite, um alle Parametersätze des Systems anzuzeigen. Diese Informationen können für Supportfälle bereitgestellt werden.

18. Verwaltung

Neustart

Neustarteinstellungen

Achtung: Wenn Sie den Sequenzmodus wählen, dann startet das Gerät 24:00 h nach N Tag[n].

Geräteneustart

Sequenzmodus :

Alle 1 [1~30] Tag[e]

Zeitplanmodus :

Son Mon Die Mit Don Fre Sam

Zeit 00:00 [hh:mm]

Speichern Jetzt neu starten

Wiederherstellen

Alle Werte auf Werkseinstellungen zurücksetzen ausser

Netzwerk Einstellungen Sommerzeit

Wiederherstellen

Dateien exportieren

Exportiere Sommerzeit Konfigurationsdatei Export

Konfigurationsdatei exportieren Export

Datei-Upload

Update Sommerzeit Einstellungen Durchsuchen... Hochladen

Backup Einstellungen uploaden Durchsuchen... Hochladen

Firmware update

Wähle Firmware-Datei Durchsuchen...

Update

System Neustart
Drücken Sie die Schaltfläche „Jetzt neu starten“, um den Videoserver neu zu starten. Sie können alternativ einen automatisierten Geräteneustart konfigurieren. Dies kann bei Netzwerkproblemen hilfreich sein. Wir empfehlen Ihnen bei Problemen, den Videoserver im wöchentlichen Rhythmus einmal neu zu starten.

Wiederherstellen
Drücken Sie die Schaltfläche, um die werkseitigen Voreinstellungen wiederherzustellen. Alle bisher getätigten Einstellungen gehen hiermit verloren.

Datei exportieren
Drücken Sie die Schaltfläche, um Ihre Videoservereinstellung in eine Datei zu exportieren.Ebenso kann die Sommerzeit Konfigurationsdatei exportiert und gesichert werden.

Datei-Upload
Drücken Sie „Durchsuchen…“ und wählen Sie die passende Konfigurationsdatei aus.
Dannach drücken Sie „Hochladen“ und warten bis die Einstellungen wiederhergestellt wurden.

Firmware Update
Hier ist es möglich, analog zum Update mit dem Installationsassistenten, die Firmware des Videoservers auf den neuesten Stand zu bringen. Die aktuellste Firmware ist unter www.abus-sc.com erhältlich. Wählen Sie die Update-Datei (*.pkg) aus, und drücken Sie die Schaltfläche UPDATE. Das Update nimmt eine kurze Zeit in Anspruch. Nach dem anschließenden Neustart des Videoservers wird diese mit der neuen Firmware in Betrieb gesetzt.

Trennen Sie auf keinen Fall den Videoserver vom Strom währrend eines Firmwareupdates. Es besteht die Gefahr einer irreparabelen Beschädigung.
Ein Firmwareupdate kann bis zu 10 Minuten in Anspruch nehmen.

19. Wartung und Reinigung

19.1 Funktionstest

Überprüfen Sie regelmäßig die technische Sicherheit des Produkts, z.B. Beschädigung des Gehäuses.

Wenn anzunehmen ist, dass ein gefahrloser Betrieb nicht mehr möglich ist, so ist das Produkt außer Betrieb zu setzen und gegen unbeabsichtigten Betrieb zu sichern.

Es ist anzunehmen, dass ein gefahrloser Betrieb nicht mehr möglich ist, wenn

- das Gerät sichtbare Beschädigungen aufweist,
- das Gerät nicht mehr funktioniert und
- nach längerer Lagerung unter ungünstigsten Verhältnissen oder
- nach schweren Transportbeanspruchungen.

Das Produkt ist für Sie wartungsfrei. Es sind keinerlei für Sie überprüfende oder zu wartende Bestandteile im Inneren des Produkts, öffnen Sie es niemals.

19.2 Reinigung

Reinigen Sie das Produkt mit einem sauberen trockenen Tuch. Bei stärkeren Verschmutzungen kann das Tuch leicht mit lauwarmem Wasser angefeuchtet werden.

Achten Sie darauf, dass keine Flüssigkeiten in das Geräteinnere kommen, dadurch wird das Gerät zerstört. Verwenden Sie keine chemischen Reiniger, dadurch könnte die Oberfläche des Gehäuses angegriffen werden

20. Entsorgung

Geräte die so gekennzeichnet sind, dürfen nicht über den Hausmüll entsorgt werden. Entsorgen Sie das Produkt am Ende seiner Lebensdauer gemäß den geltenden gesetzlichen Bestimmungen.
Bitte wenden Sie sich an Ihren Händler bzw. entsorgen Sie die Produkte über die kommunale Sammelstelle für Elektroschrott.

21. Technische Daten

Typennummer	TVIP40000
Kameratyp	Videoserver
Auflösung	QCIF,CIF,4CIF,D1 176x144 - 720x576 (Zwischenschritte frei wählbar)
Bildelemente (total)	720x576
Bildelemente (effektiv)	720x576
Digitaler Zoom	4 x
Bildkomprimierung	H.264, MPEG-4, MJPEG
Bildrate	H.264 720X480@30FPS, 720x576@25FPS
	MPEG-4 720X480@30FPS, 720x576@25FPS
	MJPEG 720X480@30FPS, 720x576@25FPS
Videonorm	PAL, NTSC
Anzahl paralleler Streams	4
Anzahl maximal User	10
Bewegungserkennung	3 Zonen
Vor- / Nachalarmspeicher	Ja
Bild-Overlay	Datum, Kameraname, Privatzonen
Alarmeingang (NO/NC)	1
Schaltausgang	1 (12VDC@400mA)
Audio	Audioausgang (Speaker Out), Audioeingang, 2-Wege-Audio
Alarmmeldung	E-Mail / FTP / HTTP-Benachrichtigung / Relaisausgang / NAS Laufwerk / SD-Karte
Unterstützte Browser	Mozilla Firefox oder Internet Explorer 6.x und höher
Unterstützte Software	eytron VMS, ONVIF Unterstützung
SD-Karte	max. 32GB (SD/SD-HC)
RS-485 Anschluss	ja
PTZ-Protokolle	Pelco D, Pelco P, LiLin, Samsung scc643, DynaDome / SmartDome
Netzwerkanschluss	RJ-45 Ethernet 10/100 Base-T mit PoE
Netzwerkprotokolle	IPv4, IPv6, TCP/IP, HTTP, UPnP, RTSP/RTP/RTCP, IGMP, SMTP, FTP, DHCP, NTP, DNS, CoS, QoS, SNMP, 802.1X
Verschlüsselung	HTTPS SSLv3
Zugriffsschutz	IP-Adressfilter, Benutzername, Passwort, 3 Berechtigungsstufen
Spannungsversorgung	12 VDC ,24 VAC, 802.3af PoE
Stromverbauch	Max. 5,0 Watt
Betriebtemperatur	0°C ~ 55°C
Abmessungen (BxHxT)	75 x 35 x 150 mm
Zertifizierungen	CE, RoHS, C-Tick

22. URL Kommandos

Für die Kunden, die bereits über ihre eigene Webseite oder Web-Steuerungs-Anwendung verfügen, kann der Videoserver über URLs leicht integriert werden. In diesem Abschnitt werden die Kommandos im URL-Format des Videoservers aufgeführt. Die Erläuterungen sind im Anhang der Anleitung in englischer Sprache aufgeführt.

23. GPL Lizenzhinweise

Wir weisen auch an dieser Stelle darauf hin, dass der Videoserver TVIP40000 u.a. Linux-Software-Programme enthalten, welche ausschließlich unter der GNU General Public License (GPL) lizensiert werden. Um eine GPL-konforme Verwendung der Programme sicherzustellen, verweisen wir auf die Lizenzbedingungen der GPL.

Lizenztext

Der Lizenztext zur GNU General Public Licence ist auf der beiliegenden Software CD oder auf der ABUS Security-Center Homepage unter
http://www.abus-sc.de/DE/Service-Downloads/Software?q=GPL
einzusehen.

Source Code

Die verwendeten Sourcecodes sind auf der ABUS Security-Center Homepage unter
http://www.abus-sc.de/DE/Service-Downloads/Software?q=GPL
zum kostenfreien Download bereitgestellt.

Lauffähigkeit des Gesamtsystems

Die zum Download angebotenen Software Pakete (Source Codes) ermöglichen es nicht, ein funktionierendes Gesamtsystem zu errichten. Dazu fehlen verschiedene Software-Anwendungen und die für das Videoserver-System entwickelte Hardware.

24. Technologie Lizenzhinweise

H.264, MPEG-4 AAC Technology

THIS PRODUCT IS LICENSED UNDER THE H.264, MPEG-4 AAC AUDIO PATENT LICENSE. THIS PRODUCT MAY NOT BE DECOMPILED, REVERSE-ENGINEERED OR COPIED, EXCEPT REGARD TO PC SOFTWARE, YOU MAY MAKE SINGLE COPIES FOR ARCHIVAL PURPOSES. FOR MORE INFORMATION, PLEASE REFER TO HTTP://WWW.VIALICENSING.COM.

H.264, MPEG-4 Visual Technology

THIS PRODUCT IS LICENSED UNDER THE H.264, MPEG-4 VISUAL PATENT PORTFOLIO LICENSE FOR THE PERSONAL AND NON-COMMERCIAL USE OF A CONSUMER FOR (i) ENCODING VIDEO IN COMPLIANCE WITH THE MPEG-4 VISUAL STANDARD ("MPEG-4 VIDEO") AND/OR (ii) DECODING MPEG-4 VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL AND NON-COMMERCIAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED BY MPEG LA TO PROVIDE MPEG-4 VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION INCLUDING THAT RELATING TO PROMOTIONAL, INTERNAL AND COMMERCIAL USES AND LICENSING MAY BE OBTAINED FROM MPEG LA, LLC. SEE HTTP://WWW.MPEGLA.COM.

AMR-NB Standard

THIS PRODUCT IS LICENSED UNDER THE AMR-NB STANDARD PATENT LICENSE AGREEMENT. WITH RESPECT TO THE USE OF THIS PRODUCT, THE FOLLOWING LICENSORS' PATENTS MAY APPLY:

TELEFONAKIEBOLAGET ERICSSON AB: US PAT. 6192335; 6275798; 6029125; 6424938; 6058359. NOKIA CORPORATION: US PAT. 5946651; 6199035. VOICEAGE CORPORATION: AT PAT. 0516621; BE PAT. 0516621; CA PAT. 2010830; CH PAT. 0516621; DE PAT. 0516621; DK PAT. 0516621; ES PAT. 0516621; FR PAT. 0516621; GB PAT. 0516621; GR PAT. 0516621; IT PAT. 0516621; LI PAT. 0516621; LU PAT. 0516621; NL PAT. 0516621; SE PAT 0516621; US PAT 5444816; AT PAT. 819303/AT E 198805T1; AU PAT. 697256; BE PAT. 819303; BR PAT. 9604838-7; CA PAT. 2216315; CH PAT. 819303; CN PAT. ZL96193827.7; DE PAT. 819303/DE69611607T2; DK PAT. 819303; ES PAT. 819303; EP PAT. 819303; FR PAT. 819303; GB PAT. 819303; IT PAT. 819303; JP PAT. APP. 8-529817; NL PAT. 819303; SE PAT. 819303; US PAT. 5664053. THE LIST MAY BE UPDATED FROM TIME TO TIME BY LICENSORS AND A CURRENT VERSION OF WHICH IS AVAILABLE ON LICENSOR’S WEBSITE AT HTTP://WWW.VOICEAGE.COM

ABUS
Security Tech Germany

eyseo.ip

TVIP40000

User Manual

Version 10/2010

Original English user manual. Keep for future use.

Introduction

Dear Customer,

Thank you for purchasing this product.

This product meets the requirements of the applicable European and national guidelines. The corresponding declarations and documents can be obtained from the manufacturer (www.abus-sc.com).

To maintain this condition and to ensure risk-free operation, you as the user must observe these operation instructions!

Before initial start-up, read through the complete operating instructions observing operating and safety instructions.

If you have any questions, please contact your installer or your local dealer!

Disclaimer

This user manual was prepared with greatest care. If you should notice omissions or inaccuracies, please inform us about these on the back of this manual given address.
The ABUS Security-Center GmbH assumes no liability for technical and typographical faults and reserves the right to make at any time modifications to the product or user manual without a previous announcement.
The company is not liable or responsible for direct and indirect subsequent damages which are caused in connection with the equipment, the performance and the use of this product.
No guarantee for the content of this document is taken.

Icon explanation

A flash in the triangle is used if there is danger for the health, e.g. by an electric shock.

An exclamation mark in the triangle points to an important note in this user manual which must be minded.

This symbol can be found when you are to be given tips and information on operation.

Important safety advice

The warranty will expire for damage due to non-compliance with these operating instructions. ABUS will not be liable for any consequential loss!

ABUS will not accept liability for damage to property or personal injury caused by incorrect handling or non-compliance with the safety-instructions.
In such cases the warranty will expire.

Dear customer,
The following safety instructions are intended not only for the protection of your health, but also for the protection of the device. Please read through the following points carefully:

- There are no parts on the inside of the product which need to be serviced. Apart from this, the license (CE) and the guarantee/warranty will lapse if you open/take the product apart.
- The product will be damaged even it falls from a low height.
- This device can be used in internal area.
- At the installation of the product please take care that direct sunlight cannot fall onto the image sensor of the device. Please follow the installation instructions in the corresponding chapter of this user manual.

Avoid using the device under the following unfavorable ambient conditions:

- wetness or excessive air humidity
- extreme cold or heat
- direct sunlight
- dust or combustible gases, vapors or solvents
- strong vibration
- strong magnetic fields, such as those found in the vicinity of machinery or loudspeakers
- the video server may not be installed on unstable surfaces

General safety instructions:

- Do not leave packaging material lying around carelessly. Plastic/ foil/bags and polystyrene parts etc. could become dangerous toys for children.
- For safety reasons don't give the video server into child hands due to them being able to swallow small parts.
- Please do not insert objects through the openings into the device.
- Use only accessories which are specified by the manufacturer.
  Please do not connect incompatible parts to the device.
- Please pay attention to the safety instructions and user manuals of the other connected devices.
- Check the device for damages before installation. If this should be the case please do not use it.
- Please adhere to the operational voltage limitations listed in the technical data. High voltage could destroy the device and pose a health hazard (electric shock).

Safety advice

1. Mains supply: Power supply 110 - 250VAC, 50/60Hz / 12VDC, 1,5A (included in package content) Operate this product only from the type of power supply indicated on the marking label. If you are not sure of the type of power supplied to your home, consult your local power company. Disconnect the product from the mains before you start any maintenance or installation procedures.

2. Overloading
   Do not overload a wall outlet, extension cord or adapter as this may result in electric fire or shock.

3. Cleaning
   Disconnect the product from the wall outlet before cleaning. Use a light damp cloth (no solvents) to dust the product.

Warnings

Follow all safety and operating advises before starting-up the device!

1. Follow these directions in order to avoid damage of the power cord or plug:
   - Do not modify or process the power cord or plug arbitrarily.
   - Do not bend or twist the power cord.
   - Make sure to disconnect the power cord holding the plug.
   - Keep heating appliances as far as possible from the power cord in order to prevent the cover vinyl from melting.

2. Follow these directions. Failure to follow any of them may cause electrical shock:
   - Do not open the main body, except for installing the HDD.
     Disconnect the product from the mains before you start.
   - Do not insert metal or inflammable objects inside the product.
   - In order to avoid any damage during lighting use a surge protection.

3. Do not use the product when it is out of order. If you continue to use the product when defective, serious damage can be caused to it. Make sure to contact your local product distributor if the product is out of order.

During the installation into an existing video surveillance system make sure that all devices are disconnected from the low and supply voltage circuit.

If in doubt allow a professional electrician to mount, install and wire-up your device. Improper electrical connection to the mains does not only represent at threat to you but also to other persons.
Wire-up the entire system making sure that the mains and low voltage circuit remain separated and cannot come into contact with each other in normal use or due to any malfunctioning.

Unpacking

While you are unpacking the device please handle it with utmost care.

If you notice any damage of the original packaging, please check at first the device.
If the device shows damages, please contact your local dealer.

Inhaltsverzeichnis

Intended use

For a detailed description of functions, refer to Chapter 4, “Initial start-up".

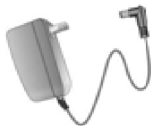
Any other use than that described above can lead to damage to the product and in addition involve other risks. This does not include operation for other applications and would in case of doing so the guarantee and any related liability will lapse. This is also the case if any unauthorized changes or additions have been made to the product.

Please read through the entire manual carefully before putting this product into operation. This operating manual contains guidelines that are important for correct mounting and operating.

1. Scope of delivery

ABUS D1 Video server
TVIP40000

Power supply



Mounting bracket

Quickguide

Software CD
including user manual

2. Installation

Make sure that all previous listed accessories were included in scope of delivery. In order to operate the video server an Ethernet network cable is necessary. The cable has to comply with specifications of UTP categories 5 (CAT 5) and must not exceed 100 meters of length.

2.1 Power supply

Before you start the installation make sure that the mains voltage and the nominal voltage of the video server correspond.

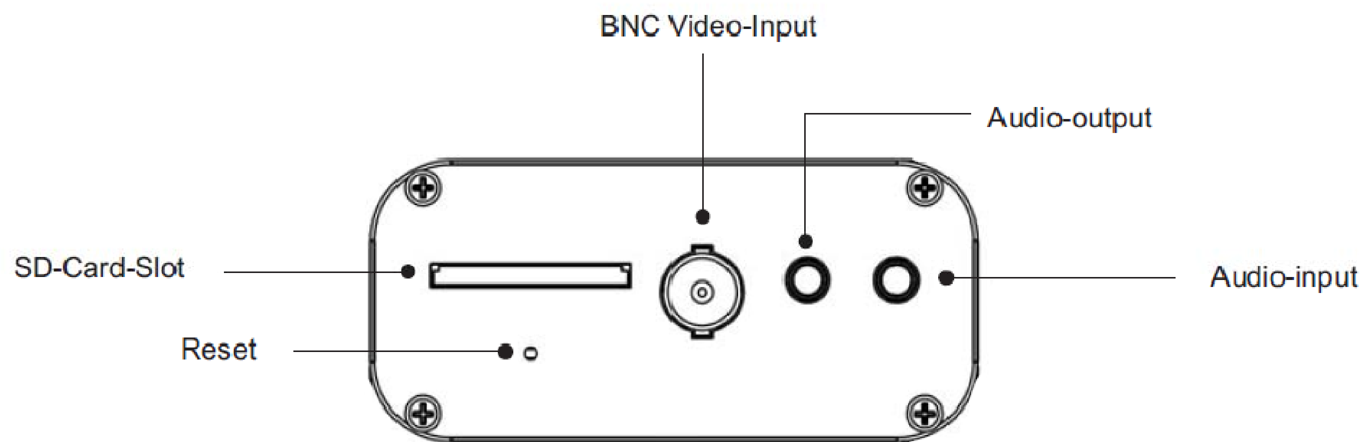
2.2 Installing the video server

To install the video server on the wall, you will need the mounting brackets and screws included in the scope of delivery.

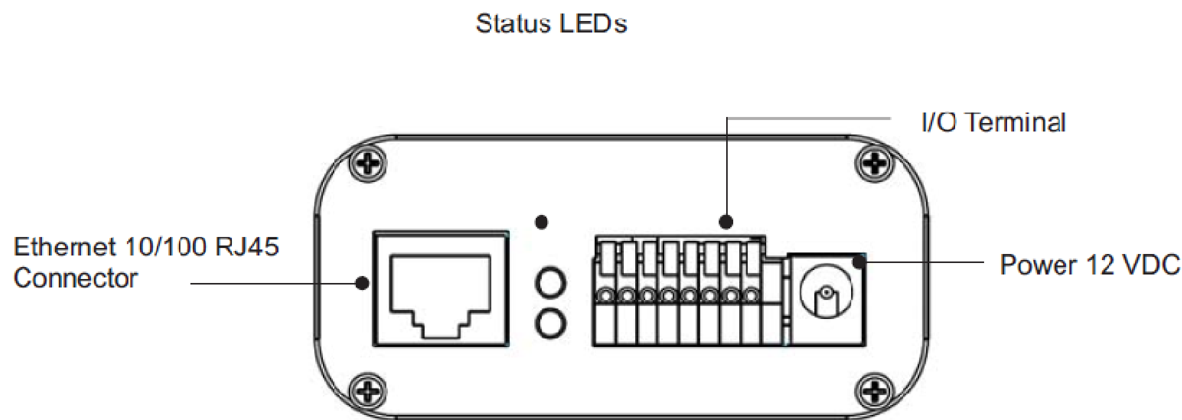
ATTENTION!
Make sure to disconnect the video server from the power supply during installation.

3. Video server description

3.1 Front view

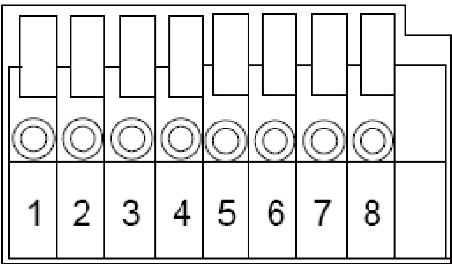


3.2 Rear view

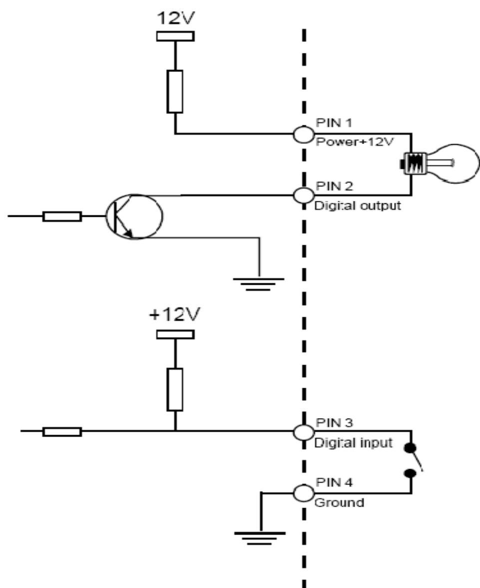


3.3 Alarm inputs and digital outputs

PIN	Descritption
1	+12V Output
2	Digital output
3	Digital input
4	Ground
5	24V AC input
6	24V AC input
7	RS-485 +
8	RS-485 -



3.4 Gate input / output ans status display



Status LED description:

Status / LED colour	Green	Red
System start	Off	On
Video server turned off	Off	Off
Network works (heartbeat)	1/s	On
Network problem	Off	On
Firmware update	1/s	0.1/s
Restoring factory settings	0.1/s	0.1/s

In order to **reboot** the video server or restore the factory settings press the reset button. Use an appropriate small tool.

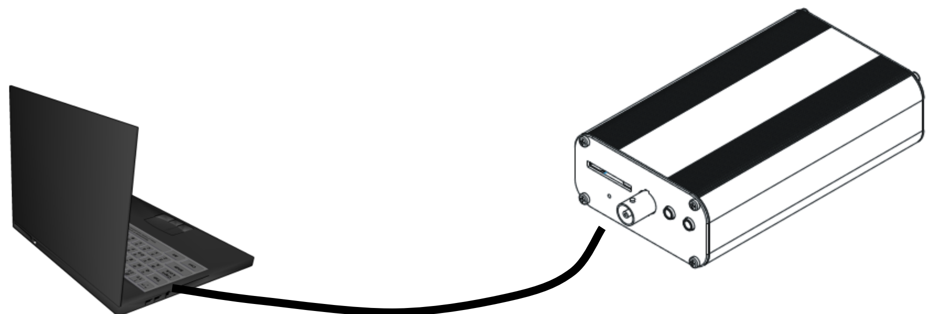
Video server reboot: Press the reset button once and wait until the video server to restart.

Restore factory settings: Press and hold the reset button for approx. 30 seconds until the status LEDs start flashing. All settings will be reset to factory default.

4. Initial start-up

Direct connection between video server and PC / laptop

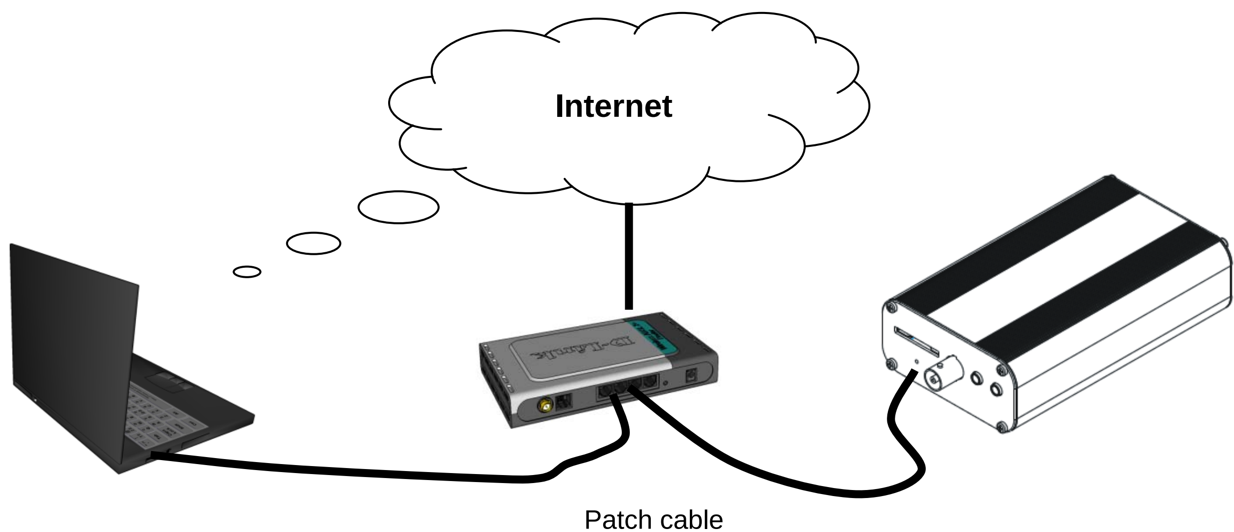
1. Make sure to use a crossover network cable
2. Connect the cable with the Ethernet port of the PC / Laptop and the video server
3. Connect the power supply to the video server
4. Configure the IP address of the PC / Laptop to 169.254.0.1
5. Continue with point 5.1 in order to finish the initial installing and build-up a connection to the video server



① Crossed Ethernet cable

Connecting the video server by using a router / switch

1. Make sure to use a pair of patch cables
2. Connect the cable with Ethernet port of the PC / laptop with the router / switch.
3. Connect the cable with the network cable and with the router / switch.
4. Connect the power supply to the video server
5. If there is a name server (DHCP) available in your network then set the IP address of your PC / laptop to “automatically receive IP address”
   If there is no name server (DHCP) available set the IP address of your PC / laptop to 169.254.0.1
6. Continue with point 5.1 in order to finish the initial installing and build-up a connection to the video server



Patch cable

4.1 First video server access

The first video server access takes place by using the program „Installation Wizard 2“.
After starting the wizard it will automatically search the network for all connected EyeseoIP network video servers and video servers.

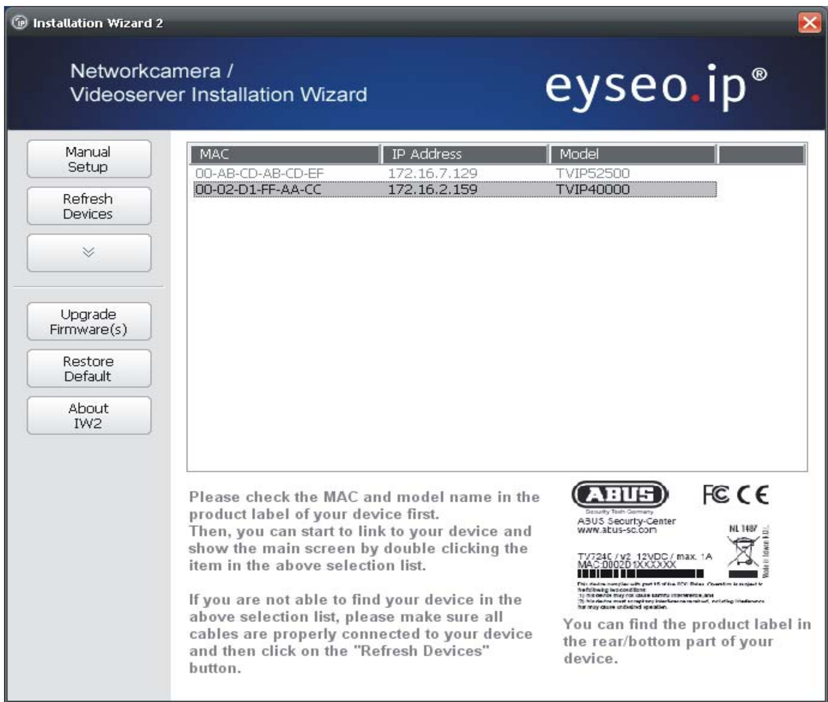
You can find the program on the on the CD at **CD-ROM\Tools\EyseoIP Tools**

Install the program on your PC and start it. The wizard will automatically search your network for EyseoIP video server.

The IP address at factory default is **169.254.0.99**. Without using the installation wizard you can only connect to the video server if the IP address of the PC is between 169.254.0.1 and 169.254.0.98.

If a DHCP server is active in your network the IP address for your PC and video server will be set automatically.

Start now the installation wizard. If no DHCP server is active the installation wizard adds a virtual IP address in the range of 169.1254.0.xx. As long as the installation wizard is active you can access the network video server by using the virtual IP address. We recommend adjusting immediately the video servers network settings to the IP settings of the PC’s network.



After closing Installation wizard 2 the additional virtual IP adress will be removed. If IP-Video server’s IP address is still in a different IP area then the one from your PC the video server access is no longer possible.

4.2 Connecting to the video server by using a web browser

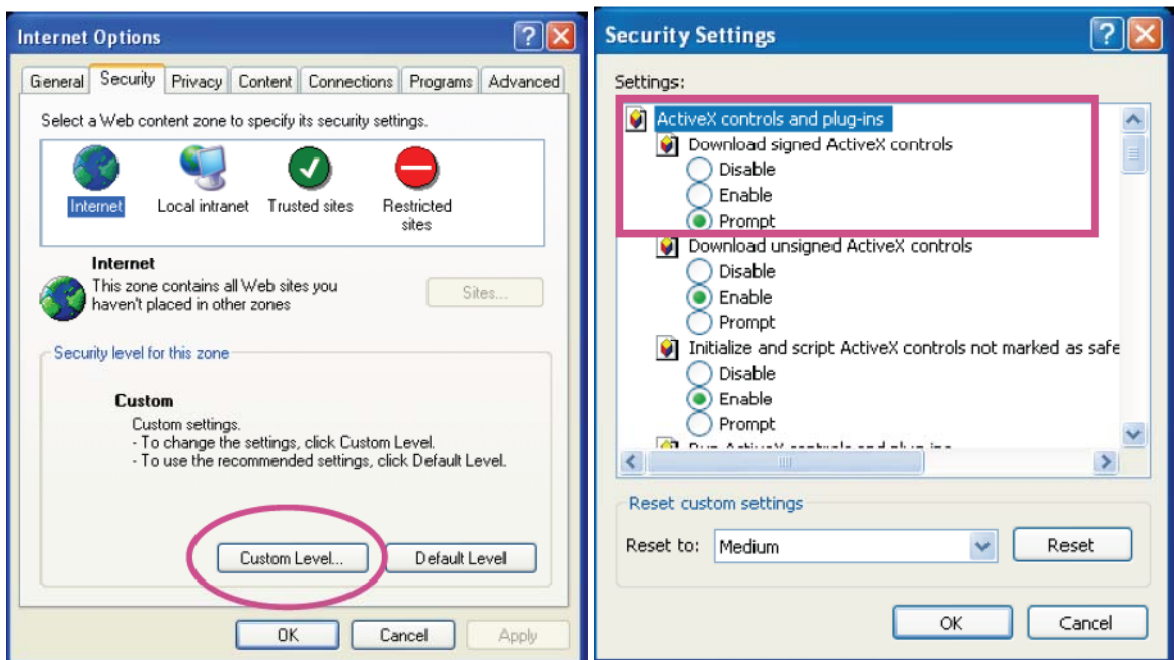
If connecting to the video server by using Mozilla Firefox or Netscape a QuickTime stream will be displayed. This requires that QuickTime from Apple is installed

In order to show the video stream when using Microsoft Inter Explorer a video plug-in is required. This will be installed when connecting to the video server. A window will appear asking you to install the plug-in. Press the install button to continue an install the plug-in. Depending on the security setup of the Internet Explorer the installation might be blocked. In this case you need to adjust the security settings.

4.3 Installing the Active-X plug-in

For Mozilla Firefox or Netscape users, your browser will use Quick Time to stream the live video. If you don't have Quick Time on your computer, please download it first, then launch the web browser.

4.4 Adjusting the security settings



NOTICE!
The security settings of the Internet Explorer can prevent displaying the video stream. Change at „Extras/Internet Options/Security" to a lower level. Make sure to activate the ActiveX control elements at "Custom Level".

4.5 Password authentication

At factory default there is no admin password set for accessing the video server. For security reasons the administrator should immediately set a password after the initial setup. After setting an admin password the video server will request for every access a username and password.

The permanent default username for the admin will be **„root"** and cannot be changed. The only way to reset the password if it is forgotten is to reset the video server to factory default settings.

In order to access the video server enter username “root” and the before defined password.

-> After successful authentication you will connect to the video server and a video stream will be displayed.

4.6 Connecting to the video server by using a RTSP player

You can display the MPEG-4 video streams by connecting to the video server with a RTSP capable media player. Following free media players support RTSP:

- VLC Media Player
- Real Player
- QuickTime Media Player

The RTSP address has to be entered as following:

rtsp://<IP-address of the network video server>:<rtsp Port>/<Name of the video stream >

How to change the name of the video stream will be explained further on.

Example:
rtsp://192.168.0.99:554/live.sdp

4.7 Connecting to the network video server by using a mobile phone

Make sure that your mobile phone is able to establish a internet connection. Furthermore the mobile phone has to have an RTSP capable media player like:

- Real Player
- Core Player

More information you can find in chapter “RTSP-Transmission”.

Please notice that limited access can occur, due to low mobile network bandwidth. We recommend following settings to optimize the video stream:

Video compression	MPEG-4
Resolution	176x144
I Frame	1 Second
Video quality (constant bit rate)	40 Kbit / Second
Audio Compression (GSM-AMR)	12.2 Kbit / Second

If the media player does not support the RTSP authentication, then deactivate this option in the RTSP settings of the video server.

The RTSP address has to be entered as following:

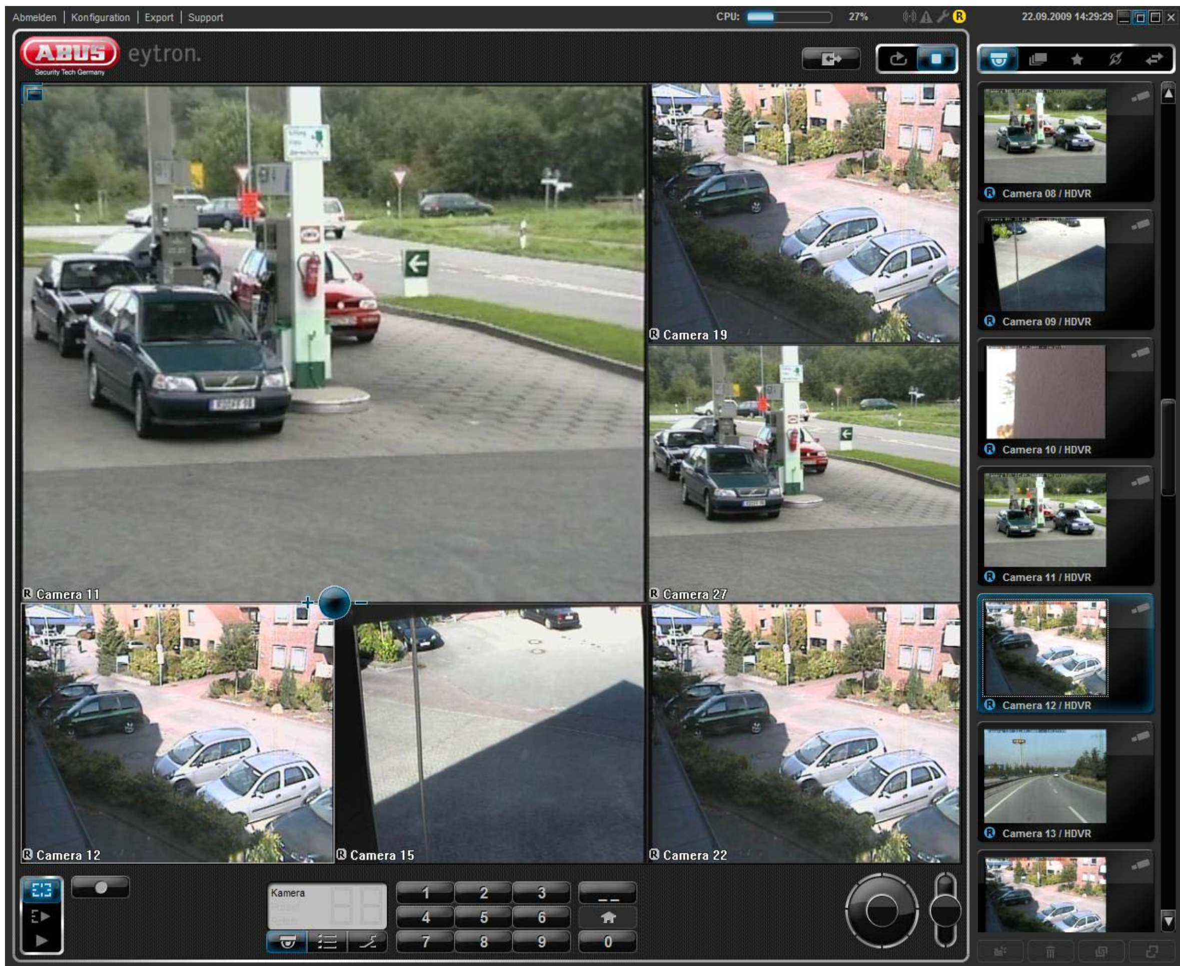
rtsp://<IP-address of the video server >:<rtsp Port>/<Name of the video stream >

How to change the name of the video stream will be explained further on.

Example:
rtsp://192.168.0.99:554/live.sdp

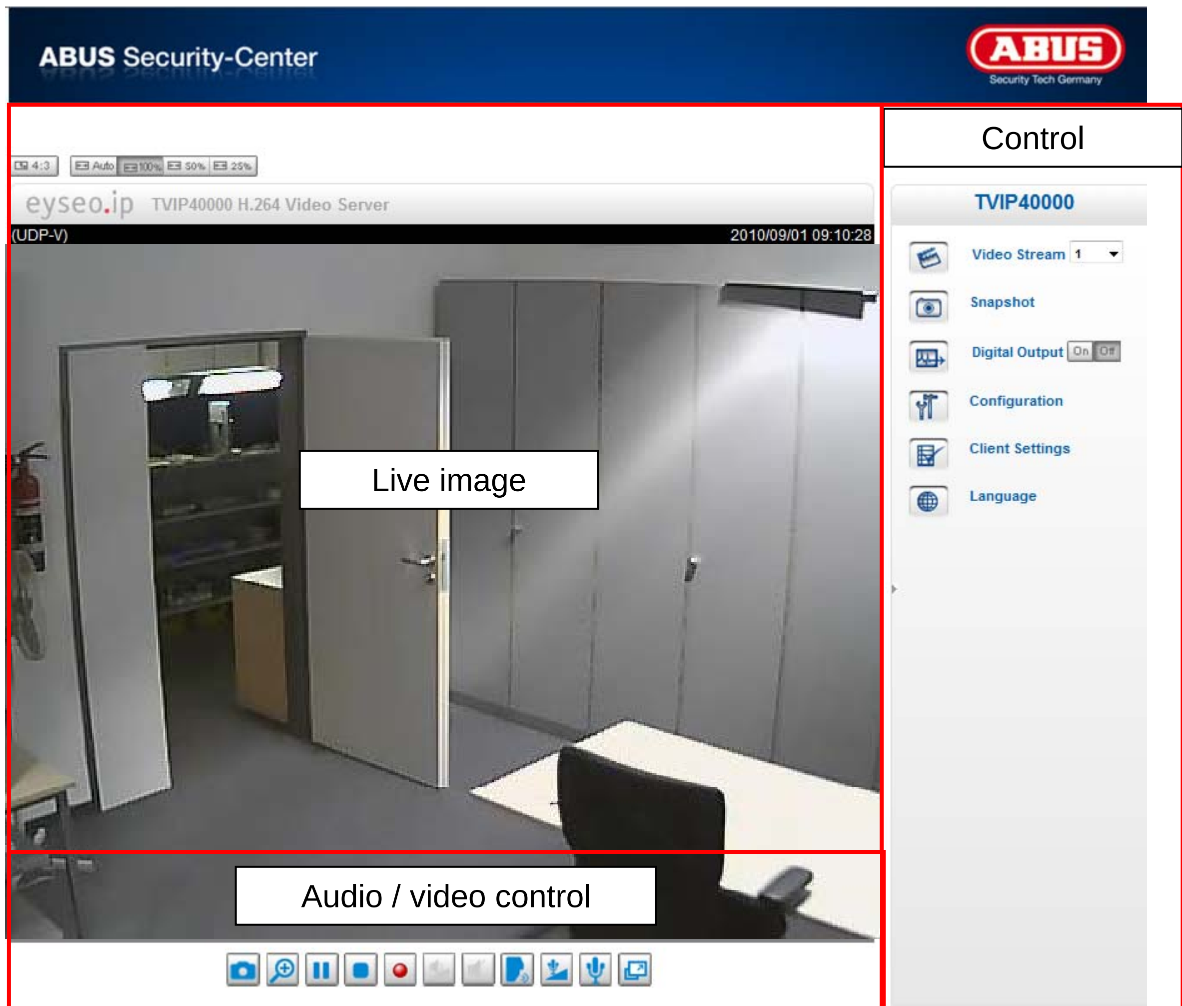
4.8 Connecting to the video server by using eytron VMS Express

The included CD contains the free recording software eytron VMS Express. This software enables you to connect and display to several IP video servers and record these. Further information can be found in the manual of the software located on the CD.



5. User functions

Open the main menu on the video server. The interface is divided into the following main areas:



Live image

- Change the zoom level by pressing the mouse scroll button.
- Click in the live picture to take over control of an analogue pan/tilt camera directly.

Video server control

Video Stream

Select from video streams 1 – 4 to view the live image.

Snapshot

Create a snapshot (without ActiveX plug-in).

Digital Output

Switch the digital output on and off manually.

Configuration

Configure the video server (administrator settings).

Client Settings

Configure the client settings; you can find detailed information on the following pages.

Language

Set the interface language.

Pan/tilt/zoom control

Use the control buttons to control the digital and mechanical pan/tilt/zoom function.

Variable view sizes

Using these buttons, you can choose from three different zoom levels for the live picture (100%, 50% and 25%). You can also adjust the live picture to automatically fit the current browser size. Do do this, select the “AUTO” option.

Screen ratio

Press the “4:3” button to set the page ratio of the live picture to 4:3.

Show/hide menu

5.1 Audio / video control

Variable view sizes

The web browser displays a new window containing the snapshot. To save the image file to your PC, right-click the image and select “Save As”.

Digital zoom and snapshot

Click on the magnifying glass icon underneath the video server view. The control panel for the digital zoom appears. Disable the “Disable Digital Zoom” box and change the zoom factor with the slider.

Start / stop live image view

The live stream can be stopped (paused) or exited. In both cases, the live stream can be continued by pressing the play symbol.

Local recording

A recording on the local hard disk can be started or stopped here. You can configure the recording path under “Client Settings”.

Adjust the volume

Press to manually set the audio output level.

Audio On / Off

Talk

As long as this button is pressed, the audio signals from the PC are transmitted to the audio output of the video server.

Microphone volume

Press to manually adjust the level for the audio input of the video server.

Mute

Press to switch the audio input of the video server on and off.

Full-screen

Activates the full-screen view. The live image on the video server is shown on the entire screen.

5.2 Client settings

The user settings are saved on the local computer. The following settings are available:

Media Options Allow the user to disable the audio or video function.

Protocol Options Allows a connection protocol to be selected between the client and the server.
The following protocol options are available for optimising the application: UDP, TCP, HTTP.

The UDP protocol gives you a larger number of audio and video streams in real time. However, some data packets can be lost due to the large data volume in the network. Pictures may be unclear in this case.
The UDP protocol is recommended if you have no special requirements.

With the TCP protocol, fewer data packets are lost and the video display is more accurate. The disadvantage of this protocol is that the realtime stream is worse than with the UDP protocol.

Select the HTTP protocol if the network is protected by a firewall and only the HTTP port (80) is to be opened.

The selection of the protocol is recommended in the following order: UDP – TCP – HTTP.

MP4 Saving Options: Here, you can modify the data path to save the data immediately. Activating the "Add date and time suffix to filename" option generates files under the following name:

CLIP_20091115-164403.MP4
FileExtensionName_YearMonthDay-HourMinuteSecond.MP4

MP4 Saving Options

Folder: c:\recordings Browse...

File name prefix: CLIP

☑ Add date and time suffix to file name

Save

The recorded data can be played back using an MP4-compatible video player (e.g. VLC Media Player).

6. Administrator Settings

6.1 System

Only the administrator has access to the system configuration. The following sections explain each of the elements in the left-hand column. Specific tasks on the Options page are printed in bold. The administrator can enter the URL under the picture to go directly to the pictures page of the configuration.

ABUS Security-Center
ABUS Security Tech Germany

Configuration
System
Security
HTTPS
SNMP
Network
DDNS
Access list
Audio and video
Motion detection
Camera tampering detection
Camera control
Application
Recording
Local storage
System log
View parameters
Maintenance
Version: 1210l

Home

System
Host name: TVIP40000 H.264 Video Server
Turn off the LED indicator

System Time
Time zone: GMT+01:00 Amsterdam, Berlin, Rome, Stockholm, Vienna, Madrid, Paris
Enable Daylight Saving Time:
Note: You can upload your Daylight Saving Time rules on Maintenance page or use the camera default value.
Keep current date and time
Synchronize with computer time
Manual
Automatic

DI and DO
Digital input: The active state is Low ; the current state detected is **High**
Digital output: The active state is Grounded ; the current state detected is **Open**

Save

"Host name" This is the text that is shown as the title on the main page.

"Turn off the LED indicator" Select this option to switch off the LED display on the video server. This prevents other persons knowing that the video server is in operation.

"Time Zone" Adjusts the time according to the selected time zone.

"Enable Daylight Saving Time" Activates daylight saving time settings in the video server. The daylight saving time settings for every time zone are already saved in the video server.

"Keep current date and time" Choose this option if you wish to keep the current date and time of the video server. An internal realtime clock stores the date and time even after the system has been switched off due to a power cut.

“Synchronise with computer time” Synchronises the date and the time of the video server with the local computer. The read-only date and time of the PC are displayed following the update.

“Manual” Sets the date and the time according to the administrator’s input. Note the date/time format when entering in the respective fields.

“Automatic” Synchronises the date and time with the NTP server via the Internet every time the video server is switched on. This is not possible if the respective time server cannot be reached.

“NTP server” Assigns the IP address or the domain name of the time server. If you leave this text box empty, the video server is connected to the default time servers.

“DI and DO” Sets the pre-defined state for the alarm input and relay output.

Do not forget to press **“Save”** in order for your changes to take effect.

6.2 Security

“Root Password” Allows users to change the administrator password by entering a new password. For security reasons, the passwords entered are shown as asterisks. After **“Save”** is clicked, the web browser prompts the administrator to enter the new password for accessing the video server.

“Add new user” Enter the new user name and password and click **“Add”**. The new user is displayed on the list of user names. Up to twenty user accounts can be configured.

“Edit users” Open the list of user names, select the user that you wish to edit, and change the required values. To apply the changes, click **“Update”**.

Root Password
Note: Leaving the root password field empty means the camera will not be protected by password.
Root Password:
Confirm root password:
Save

Manage Privilege
Operator Viewer
Digital Output:
PTZ control:
Allow anonymous viewing
Save

Manage User
Existing user name: --Add new user--
User name:
User password:
Confirm user password:
Privilege: Administrator
Delete
Add
Update

“Delete user” Open the list of user names, select a user and click **“Delete”**, to delete this user from the list.

User administration

Administrator: Complete unrestricted access to the video server.
Operator: No access to the configuration page. Can also execute URL commands (e.g. PTZ).
User: Access is restricted to the main page (live view).

Digital Output: The user group can control the alarm input and output.
PTZ control: The user group has access to the PTZ control.
Allow anonymous viewing: There is no prompt for a user name and password when the main page is displayed.

6.3 HTTPS

The HTTPS
protocol is used for encryption and for authenticating communication between the web server (video server) and browser (client PC) on the Internet. All data transmitted between the video server and client PC is encrypted using SSL. Apart from SSL encryption (compatible with all standard browsers), a source authorisation certificate is required in order to use HTTPS.

Enable HTTPS

*To enable HTTPS, you have to create and install certificate first.

☐ Enable HTTPS secure connection:

Save

Create and install certificate method

◉ Create self-signed certificate automatically

○ Create self-signed certificate manually:

○ Create certificate request and install:

Certificate Information

Status: Not installed

Property Remove

"Enable HTTPS secure connection" You can choose between unencrypted (HTTP) + encrypted (HTTPS) access or encrypted (HTTPS) access only.

If a secure HTTPS connection is enabled, the video server can be accessed using the following lines:
https:\\"IP-Adresse"
If you wish to stream using the HTTPS connection, use the following link:
https:\\"IP-Adresse":"HTTPS-Port\Live.sdp

Creating and installing a certificate

"Create self-signed certificate automatically" The pre-defined certificate in the video server is used. With this option, no settings can be made by users.

"Create self-signed certificate manually" A new certificate is generated. Specific data must be entered.

"Create certificate request and install" Select this option if you wish to generate a certificate request which is then submitted to a certificate authority. A certificate issued by a recognised certification authority (e.g. VeriSign) can also be installed on the video server.

Note: When using a "self-signed certificate", you may receive a warning message from your browser. Self-signed certificates are always classed as insecure by the browser as the source certificate and authorisation of the certification authority are both absent.

6.4 SNMP

The Simple Network Management Protocol is a network protocol that can be used to monitor and control network devices (e.g. routers, servers, switches, printers, computers etc.) from a central station. Here, the Protocol controls the communication between the monitored devices and the monitoring station. Enable this function if you are using an SNMP management server in your network. You can also access software solutions that can be installed on your PC system.

"Enable SNMPv1, SNMPv2c" Depending on your SNMP server settings, you can define the name fields of the read/write community here.

SNMP Configuration

Enable SNMPv1, SNMPv2c

SNMPv1, SNMPv2c Settings

Read/Write community: Private

Read only community: Public

Enable SNMPv3

Save

"Enable SNMPv3" If your SNMP server supports the SNMP protocol in version 3, you can execute the status query with encryption. To do this, an encryption algorithm and password for the read/write community status query must be saved in the video server and SNMP server.

6.5 Network

6.5.1 Network settings

All changes made on this page cause the system to restart in order for the changes to take effect. Make sure that the fields are correctly filled before you click "Save".

"LAN" The default is LAN. Use this setting if the video server is connected to a LAN. You also have to make other settings such as the IP address or the subnet mask.

"Obtain an IP address automatically" Every time the video server is restarted, it is assigned an IP address via a DHCP server.

"Use fixed IP address" The network data is fixed here, e.g. the IP address.

"IP address" This is required for network identification.

"Subnet mask" This defines whether the destination is in the same subnet. The default value is **"**255.255.255.0".

"Standard-Router" Gateway for transmitting pictures to another subnet. An invalid router setting prevents transmission to these destinations in different subnets. If a cross-link cable connection is available, you must enter an IP which is in the same subnet range as the video server (e.g. 192.168.0.1).

"Primary DNS" Server of the primary domain name with which the hostnames are converted into IP addresses.

"Secondary DNS" Server of the secondary domain name for generating a reserve copy of the primary DNS.

"Use UPnP" This enables Universal Plug and Play. If your operating system supports UPnP, the video server can be accessed directly via UPnP management (Windows: network environment)

Andere Geräte (1)
TVIP40000 H.264 Video Server (192.168.178.49)
Computer (1)
ABUS-PC
Kameras (1)
TVIP11550 - 000E8E21AE5D
Netzwerkinfrastruktur (1)
PMV1 UPnP/1.0 AVM FRITZ!Box Fon WLAN 7170 29.04.76

Make sure that the option "Use UPnP" is always enabled. UPnP is also used by eytron VMS to search the video server.

"UPnP port forwarding ON" Enables Universal Plug and Play port forwarding for network services. If your router supports UPnP, then port forwarding for video streams is activated automatically on the router for the video server using this option.

"PPPoE" Use this setting if the video server is connected directly to a DSL modem. You will receive a user name and password from your ISP (Internet Service Provider).

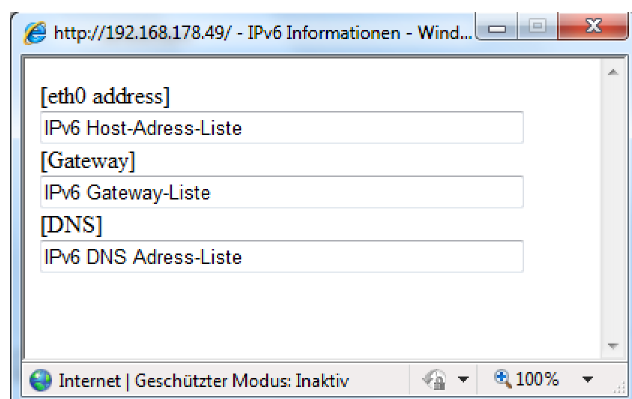
"IPv6" Use this function to work with IP addresses of generation v6.

Enable IPv6
IPv6 Information
Manually setup the IP address
Optional IP address / Prefix length / 64
Optional default router
Optional primary DNS

Please note that your network and hardware must support IPv6.

If IPv6 is enabled, the video server always waits until it is assigned an IPv6 address via DHCP.
If no DHCP server is available, set up the IP address manually.
To do this, enable "Manually setup the IP address" and enter the IP address, default router and DNS address.

"IPv6 Information" All the IPv6 information is displayed in a separate window.



If the IPv6 settings are correct, you can read all the settings in the lower window.

[eth0 address]
2001:0c08:2500:0002:0202:d1ff:fe04:65f4/64@Global
fe80:0000:0000:0000:0202:d1ff:fe04:65f4/64@Link
[Gateway]
fe80::211:d8ff:fea2:1a2b
[DNS]
2010:05c0:978d::

6.5.2 IEEE 802.1x

Activate this function if your network environment uses the standard IEEE 802.1x, a port-based access control in the network.
IEEE 802.1x improves the security of local networks.
A connection is only permitted if all certificates between the server and "client" have been verified. They are authenticated by a switch/access point, which sends queries to the RADIUS authentication server.
Otherwise no connection is made and access to the port is denied.

Please note that your network components and the RADIUS server must support the standard IEEE 802.1x.

6.5.3 HTTP

"HTTP port" This port can be different from the standard port 80 (80, or 1025 – 65535). If this port is changed, users must be informed to ensure a successful connection. Example: If the administrator changes the HTTP port of the video server with the IP address 192.168.0.99 from 80 to 8080, users have to enter "http://192.168.0.99:8080" in the web browser instead of "http://192.168.0.99".

"Secondary HTTP port" Additional HTTP port for the video server access

For the direct access to individual video streams over the web, the following access names can be configured. Access is gained via compressed JPEG images and allows web browsers (Firefox, Netscape) which cannot process ActiveX plug-ins to access the video stream directly:

"Access name for stream 1" Access name for the MJPEG stream 1
"Access name for stream 2" Access name for the MJPEG stream 2
"Access name for stream 3" Access name for the MJPEG stream 3
"Access name for stream 4" Access name for the MJPEG stream 4

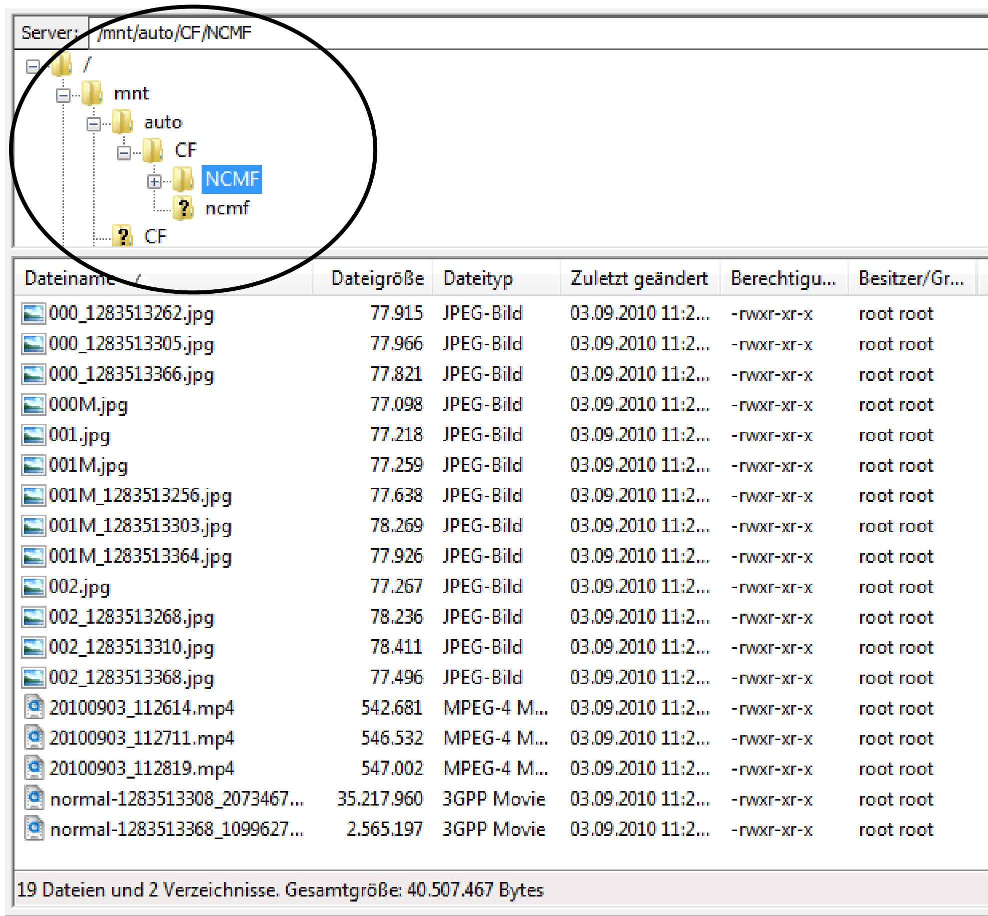
Note: Internet Explorer does not support the display of MJPEG images without Active

6.5.4 FTP

“**FTP port**” This is the internal FTP server port. It can be a different port to the standard port 21 (21, or 1025 – 65535). The video data saved on the video server can be called up directly via FTP. Use a separate FTP program for this purpose.

The address format for entering the connection data is as follows:
Server: IP address of the video server
User name: Administrator user
Password: Password of administrator
Port: FTP port of the video server

Example (with FTP program)
Server: 192.168.0.99
User name: root
Password: admin
Port: 1026



Dateiname /	Dateigröße	Dateityp	Zuletzt geändert	Berechtigu...	Besitzer/Gr...
000_1283513262.jpg	77.915	JPEG-Bild	03.09.2010 11:2...	-rwxr-xr-x	root root
000_1283513305.jpg	77.966	JPEG-Bild	03.09.2010 11:2...	-rwxr-xr-x	root root
000_1283513366.jpg	77.821	JPEG-Bild	03.09.2010 11:2...	-rwxr-xr-x	root root
000M.jpg	77.098	JPEG-Bild	03.09.2010 11:2...	-rwxr-xr-x	root root
001.jpg	77.218	JPEG-Bild	03.09.2010 11:2...	-rwxr-xr-x	root root
001M.jpg	77.259	JPEG-Bild	03.09.2010 11:2...	-rwxr-xr-x	root root
001M_1283513256.jpg	77.638	JPEG-Bild	03.09.2010 11:2...	-rwxr-xr-x	root root
001M_1283513303.jpg	78.269	JPEG-Bild	03.09.2010 11:2...	-rwxr-xr-x	root root
001M_1283513364.jpg	77.926	JPEG-Bild	03.09.2010 11:2...	-rwxr-xr-x	root root
002.jpg	77.267	JPEG-Bild	03.09.2010 11:2...	-rwxr-xr-x	root root
002_1283513268.jpg	78.236	JPEG-Bild	03.09.2010 11:2...	-rwxr-xr-x	root root
002_1283513310.jpg	78.411	JPEG-Bild	03.09.2010 11:2...	-rwxr-xr-x	root root
002_1283513368.jpg	77.496	JPEG-Bild	03.09.2010 11:2...	-rwxr-xr-x	root root
20100903_112614.mp4	542.681	MPEG-4 M...	03.09.2010 11:2...	-rwxr-xr-x	root root
20100903_112711.mp4	546.532	MPEG-4 M...	03.09.2010 11:2...	-rwxr-xr-x	root root
20100903_112819.mp4	547.002	MPEG-4 M...	03.09.2010 11:2...	-rwxr-xr-x	root root
normal-1283513308_2073467...	35.217.960	3GPP Movie	03.09.2010 11:2...	-rwxr-xr-x	root root
normal-1283513368_1099627...	2.565.197	3GPP Movie	03.09.2010 11:2...	-rwxr-xr-x	root root

19 Dateien und 2 Verzeichnisse. Gesamtgröße: 40.507.467 Bytes

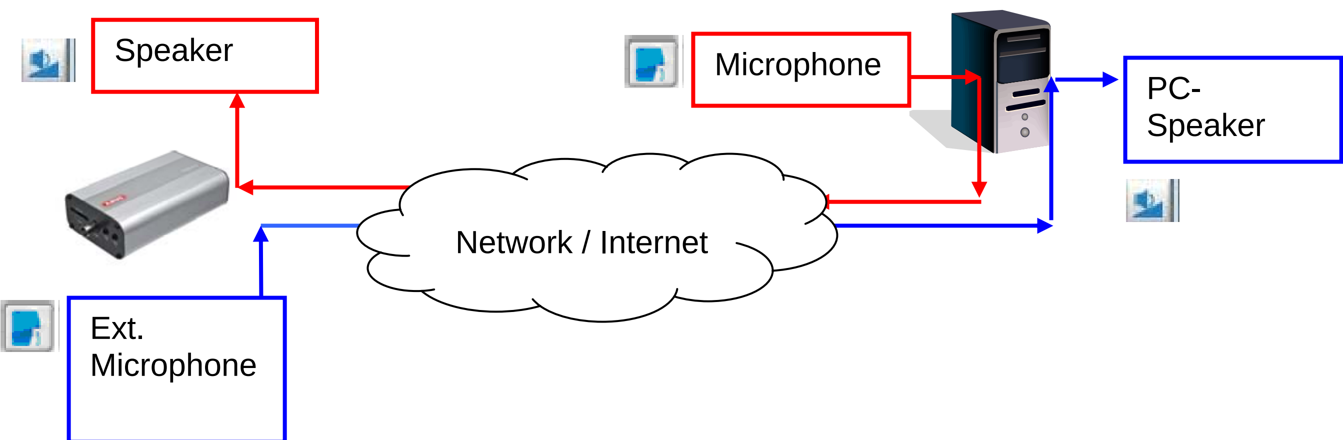
6.5.5 HTTPS

“HTTPS port” This is the port setting for the internal HTTPS port. It can be a different port to the standard port 443 (443, or 1025 – 65535). You can find further configuration options for HTTPS in section 5.5.3.

6.5.6 Two-way audio

"Two-way audio" This is the port for the two-way audio function. This port can be different from the standard port 5060 (5060 or 1025 – 65535).

To be able to use the two-way audio function, you must enable **"Video and audio"** for the selected video stream MPEG-4/H.264. MJPEG only supports the transmission of video data and is therefore not suitable for this function.



Live stream functions:

Start the audio data transmission.

Control the sensitivity of the video server audio input.

Switch off the microphone/audio input.

Click the button again to stop the audio transmission.

6.5.7 RTSP transmission

"RTSP authentication" The authentication options are: disable (standard), basic (simple) or an expanded mode (digest).

I If the RTSP authentication is enabled, the user name and password of a valid user (e.g. administrator) must be entered during the RTSP connection setup.
IMPORTANT: The RTSP authentication must be supported by the video player (e.g. Realplayer 10.5).

"Access name for stream 1" This is the access name 1 for establishing a connection from a client. The codec type must be MPEG4. Use
rtsp://<IP address>:RTSP port /<access name 1>, to establish a connection.

"Access name for stream 2" This is the access name 2 for establishing a connection from a client. The codec type must be MPEG4. Use
rtsp://<IP address>:RTSP port /<access name 2>, to establish a connection.

"Access name for stream 3" This is the access name 3 for establishing a connection from a client. The codec type must be MPEG4. Use
rtsp://<IP address>:RTSP port /<access name 3>, to establish a connection.

"Access name for stream 4" This is the access name 4 for establishing a connection from a client. The codec type must be MPEG4. Use
rtsp://<IP address>:RTSP port /<access name 4>, to establish a connection.

RTSP access with VLC:
rtsp://192.168.0.99:10052/live.sdp

“RTSP port” This port can be different from the standard port 554 (554; or 1025 to 65535). If you change it, note that the input format is analogue to the HTTP port.

“RTP port for video” This port can be different from the default port 5558. The port number must always be even.

“RTCP port for video” This port must be the “RTP port for video” plus 1.

“RTP port for audio” This port can be different from the default port 5556. The port number must always be even.

“RTCP port for audio” This port must be the “RTP port for audio” plus 1.

6.5.8 Multicast transmission

Multicast is the message transmission from a single point to a group (also known as a multiple-point connection). The advantage of multicast is that messages can be transmitted simultaneously to several recipients or a closed user group without the bandwidth of the sender increasing according to the number of recipients. When using multicast, the sender only requires the same bandwidth as a single recipient. The packets are multiplied on each network distributor (switch, router).

Multicast allows data to be sent efficiently to many recipients at the same time in IP networks. This is made with a special multicast address. In IPv4, the address range 224.0.0.0 to 239.255.255.255 is reserved for this purpose.

The following multicast settings can be configured for streams 1 - 4 in the video server.

Enable **“Always multicast”** to use multicast.

“Multicast group address” Specifies a group of IP hosts which belong to this group

“Multicast video port” This port can be different from the default port 5560. The port number must always be even.

“Multicast RTCP video port” This port must be the “Multicast video port” plus 1.

“Multicast audio port” This port can be different from the default port 5562. The port number must always be even.

“Multicast RTCP audio port” This port must be the “Multicast audio port” plus 1.

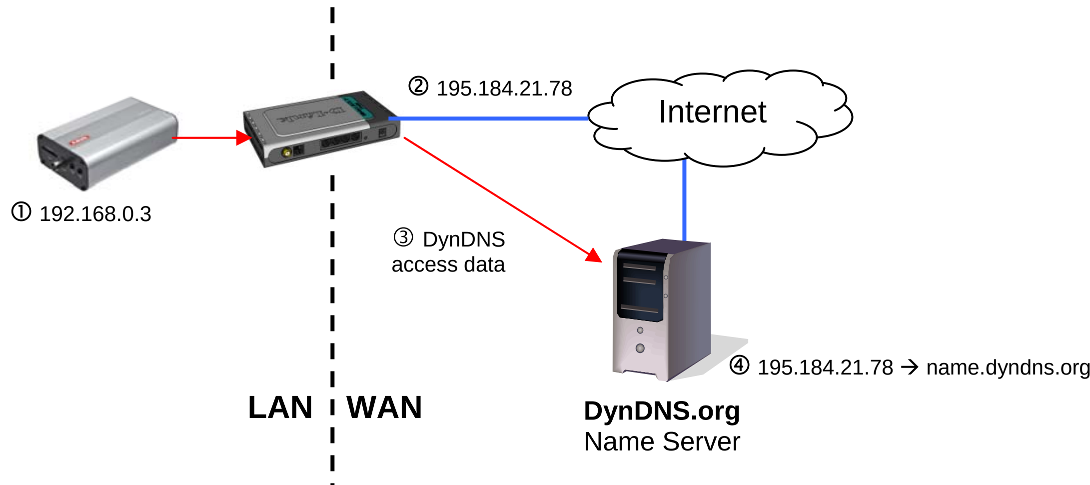
“Multicast TTL” Time to Live

If you are setting up port forwarding in a router, all ports should always be forwarded this way (RTSP + HTTP). This is imperative for successful communication.

7. DDNS

DynDNS or DDNS (Dynamic Domain Name System) is a system used for updating domain name entries in real time. The video server is equipped with an integrated DynDNS client, which updates the IP address independently via a DynDNS provider. If the video server is positioned behind a router, we recommend using the DynDNS function on the router.

The following diagram offers an overview of accessing and updating the IP address using DynDNS.



"Enable DDNS" Enables the DDNS function.

"Service providers" The provider list contains the hosts that provide DDNS services. Connect to the service provider's website to make sure that the service is available.

"Host name" This field must be completed if you want to use the DDNS service. Enter the host name registered with the DDNS server.

"User name/email" The user name and the email address must be entered in this field to set up a connection to the DDNS server or to inform users about the new IP address. Note: If you enter a "User name" in this field, you must enter a "Password" in the next field.

"Password" To be able to use the DDNS service, enter your password in this field.

DDNS: Dynamic domain name service

Enable DDNS:

Provider: Dyndns.org(Dynamic)

Host name:

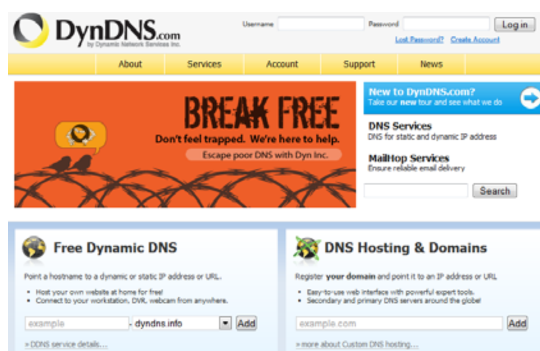
User name:

Password:

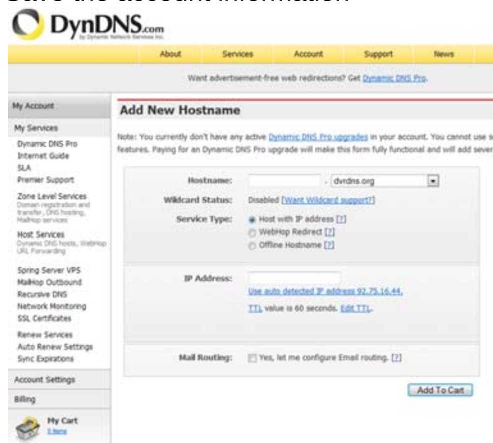
Save

7.1 Setting up a DDNS account

Set up a new account at DynDNS.org



Save the account information

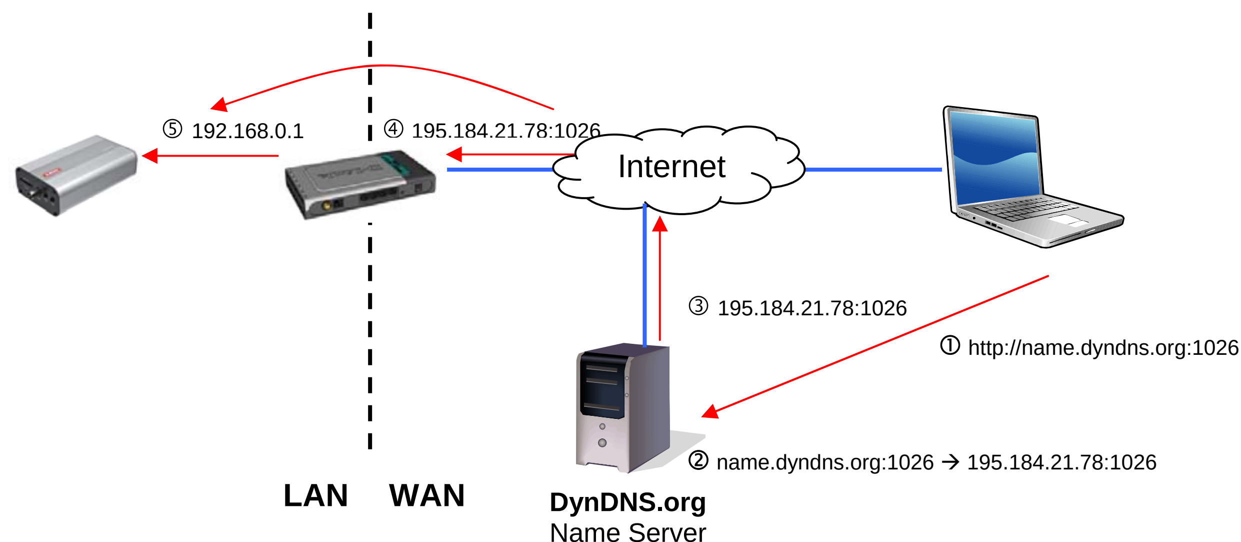


Note down your user data and enter this into the configuration of the video server.

7.2 DDNS access via a router

If your network video server is positioned behind a router, then access via DynDNS must be configured in the router. A description of the DynDNS router configuration for common router models can be found on the ABUS Security-Center website: www.abus-sc.com.

The following diagram offers an overview of accessing a video server behind a router via DynDNS.org.



Port forwarding of all relevant ports (at least RTSP + HTTP) must be set up in the router in order to use DynDNS access via the router.

8. Access list

This is where you control access to the video server using IP address lists.

"Maximum number of concurrent streaming connection(s) limited to" Number of possible simultaneous connections to the video server. Depending on the bandwidth available for the video server, it may make sense to limit the access.
"Enable access list filtering" Enables the IP address filters listed defined under "Filters"
You have two options for defining IP address filtering:

- "Allow" filter type: only IP addresses in the defined address space have access, or
- "Deny" filter type: IP addresses in the defined address space have no access.

Click **"Add"** to configure the address ranges. The following configuration options are given:

General Settings
Maximum number of concurrent streaming connection(s) limited to: 10 View Information
Enable access list filtering
Save
Filter Type
Allow Deny
Save
Filter
IPv4 access list
Add Delete
Administrator IP address
Always allow the IP address to access this device
Save

Rule: Single, Range, Network:

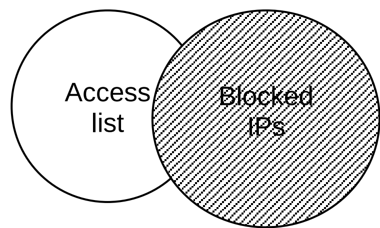
- Single: a specific IP address is added
- Range: IP address ranges from - to can be defined
- Network: IP addresses with a specific subnet mask can be defined

filter address
Rule: Single
Single
Network
Range
IP addr
OK Cancel

Example:
The IP address range from 192.168.0.1 to 192.255.255.255 should be permitted.
The following IP addresses should be blocked 192.168.1.0 to 192.168.255.255.

Result:
Access is only granted for IPs from the following range: 192.168.0.1 – 192.168.0.255.

An intersection is formed between IPs which are allowed access and denied access.



9. Audio and Video

Video Settings

Video title:

Color: Color

Modulation: Auto

Select caching stream: Stream 4

Video orientation: Flip Mirror

Overlay title and time stamp on video and snapshot.

Image Settings | Privacy Mask

Video quality settings for stream 1:

Video quality settings for stream 2:

Video quality settings for stream 3:

Video quality settings for stream 4:

Audio Settings

Mute

External microphone input: 0 dB

Audio type:

AAC:

AAC bit rate: 16 Kbps

GSM-AMR:

G.711:

Mode: pcmu

Save

“Video title” The text appears in the black bar above the video window with a timestamp. This timestamp (date and time) is provided by the integrated realtime clock of the video server.

“Colour” Choose between colour and black and white display.

“Modulation” Select between the video standard NTSC and PAL or automatic video signal recognition via the video server.

“Select caching stream” The selected video stream is used for recording the pre- and post-alarm video data (see “Application” section).

“Flip” Rotates the video horizontally. Select this option if the camera has been installed upside down.

“Mirror” Rotates the video vertically.

Select the flip and mirror options if the camera is installed on the ceiling.

“Overlay title and time stamp on video and snapshot” You can use this option to display the title and time stamp directly in the video image and snapshots. The input for “Video title” is used here.

9.1 Image Settings

“Brightness, contrast, saturation, sharpness” Adjust the values according to your lighting conditions.

Image Adjustment
Brightness: +0 Saturation: +0
Contrast: +0 Sharpness: +0
Preview Restore Save
Close

If the lighting conditions for the camera change, image settings for bad lighting conditions may compromise the image quality of videos with good lighting conditions.

To view the changed settings for the image, click “Preview”. To save the picture parameters, click “Save”. To discard your changes, click “Restore”.

9.2 Privacy masking zones

This function allows you to hide areas in the video image. You can select 5 areas of any size.

Enable this function by selecting the **“Enable privacy mask”** option.

Click **“New”** to create a new window; you can then adjust the size. Click **“Save”**, to apply the changes.

Enable privacy mask
2008/12/11 14:28:35
Window Name
1
X168 Width88
Y32 Height208
New Save

This function should not be enabled if the PTZ/ePTZ function of the camera is being used. This function can only be configured if MS Internet Explorer is used as a browser (ActiveX mode).

9.3 Basic setting:

Video options
The video server has four video streams with different quality settings available for flexible application.

- Video quality settings for stream 1:
- Video quality settings for stream 2:
- Video quality settings for stream 3:
- Video quality settings for stream 4:

Settings for streams 1, 2, 3 and 4
You can configure streams 1 – 4 in the respective menus.

The quality settings for stream 4 is determined on QCIF. Use stream 4 for streaming on mobile devices.

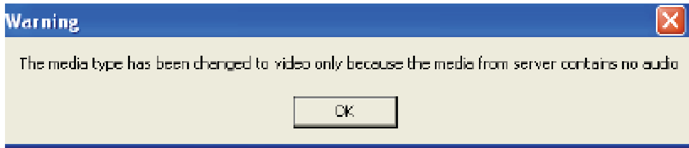
"Image compression" Select from H.264/MPEG-4/MJPEG.
"Image size" Select your desired resolution here.
"Max. image rate" Select your maximum refresh rate here.
"Key frame interval" Determines how often an Intra Frame is generated. The shorter the interval, the better the image quality, and the higher the network usage costs.
"Video quality fixed image rate" Sets the image rate at a constant value. The image quality is reduced the more complex an image is (e.g. motion).
"Fixed image quality" Sets the image quality at a constant value. The bit rate increases with the image complexity (e.g. motion).

Compression → / Recording duration ↓	**H.264**	**MPEG-4**	**MJPEG**
1 minute video sequence in D1 resolution with "good" quality	Approx. **12** MB	Approx. **14** MB	Approx. **60** MB
Storage capacity **32 GB** SD card	Approx. **43** hours	Approx. **36** hours	Approx. **9** hours

At the end of the manual you can find a detailed table with every quality setting combined with every resolution.

9.4 Audio settings

“Mute” All audio functions in the video server are deactivated. A note appears when you access the video server.



“External microphone/audio amplification” Adjust the value from +21 db to -33 db.

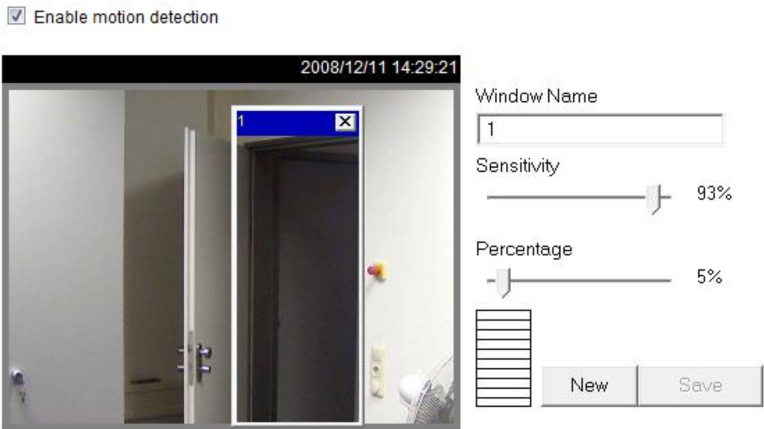
“Audio type” Select the audio type and desired bit rate. A higher value requires more bandwidth:

- **“AAC”** (Advanced Audio Coding) Special codec for audio data compression under MPEG-4/H.264.
- “**GSM-AMR”** (Global System for Mobile Communications – Adaptive Multi Rate) Voice codec in GSM mobile telephone network.
- **“G.711”** pmca/pmcu (Pulse Code Modulation).

10. Motion detection

You can activate up to three motion zones in the video server. Select “**Enable motion detection**”, to configure the function.

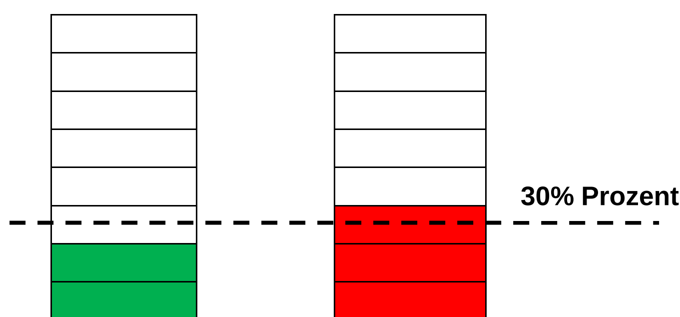
The motion detection function is only active once you have defined an action under the “Application” menu item.



“**Window Name**” The text appears at the top of the window.
“**Sensitivity**” Sensitivity in changes of picture sequence (e.g.: sensitivity high: triggering by slight picture change).
“**Percentage**” Specifies the percentage of the image that has to change for the motion sensor to be triggered.

Click “New” to add a new window. To resize the window or move the title bar, click the window frame, keep the mouse button pressed and drag the window to the required size. Close the window by clicking the “x” in the top right corner.
Click “Save” to save the window settings. A bar graph rises or falls according to the picture variation.

A green bar means that the picture variation is below the surveillance level, whilst a red bar means that the picture variation is above the surveillance level. If the bar is red, the detected window appears with a red frame. When you return to the homepage, the monitored window is hidden. As soon as motion is detected, the red frame is displayed.



Green area: Motion recognised, however alarm is not triggered.
Red area: Picture variation (motion) exceeds the limit value of 30% and triggers an alarm.

Functionality of motion detection:

Two parameters are available for configuring motion detection: **Sensitivity** and **percentage**. The figure shows how these two parameters influence motion detection.

A motion occurs, shown in the progression from figure A to figure B. The resulting pixel changes (depending on the sensitivity setting) are shown in figure C (grey). The **“Sensitivity”** setting refers to the capacity of the sensor to detect motion in the picture. The higher the set value, the more pixel changes are detected in the picture. When motion is detected, the pixel changes (depending on the sensitivity setting) are saved on the server as alarm pixels (pink areas in figure D). The **“Percentage”** value describes the percentage of the “alarm pixels” in relation to the total number of pixels in the selected area. If the specified percentage of alarm pixels is reached or exceeded, an alarm is triggered. To ensure reliable motor detection, a high sensitivity setting and low percentage value is recommended.

11. Camera tampering detection

The video server supports tampering detection. If detection is enabled, the alarm can be used as an event for a notification (see “Application”).

“Enable video server tampering detection” The sensor system is activated.

“Triggering behaviour” The period defines how long a tampering event must continue before an alarm is triggered.

The following tampering events are checked:

- Camera rotation
- Camera masking
- Camera defocussing

You can set tampering detection as a trigger in the camera function “Application/Event setup”.

12. Camera control

The video server includes an option for analogue PTZ camera control.

RS485 Settings

“Disable” RS485 control is switched off.

“PTZ camera” Here, enter the relevant parameters for the PTZ camera. The following protocols are supported: Pelco-D, Pelco-P, Samsung scc643, DynaDome/SmartDOME, Lilin PIH-7x00.
If none of these protocols are supported by your PTZ camera, select “Custom camera”.

“Transparent HTTP Tunnel” If your PTZ device supports RS485 commands via a network interface, you can select this option. Refer to the operating manual of your PTZ device for the necessary parameters.

RS485 Settings

Disable

PTZ camera

Transparent HTTP Tunnel

Camera ID: 1

PTZ driver: Pelco D protocol

Port settings:

Baud rate: 2400

Data bits: 8

Stop bits: 1

Parity bit: none

Preset Position | Custom Command

Save

Refer to the operating manual of your PTZ device for the exact PTZ commands.

"Camera ID" Defines the camera ID.
"PTZ driver" Defines the protocol of the connected PTZ device.
"Baud rate" Enter the appropriate baud rate.
"Data bits" Enter the appropriate data bits.
"Stop bits" Enter the appropriate stop bits.
"Parity bit" Defines the parity.

Preset positions and setting up a patrol

Up to 20 preset positions can be saved in the video server. Proceed as follows:

1. Move the camera picture into the desired position using the direction keys
2. Give the current position a preset name and click "Add". The name appears in the preset locations list Wiederholen Sie die
3. Repeat steps 1-2 to add more preset locations
4. Highlight the preset locations that you wish to use for a patrol, and confirm these with "Select"
5. Adjust the dwelling time for each of the preset locations if required.
6. Save your settings

To begin the patrol, press "PATROL" in the live picture of the video server. Press "STOP" to stop this).

Custom command

The "Custom Command" menu item allows you to access individual functions of your PTZ device or PTZ camera directly.
This function is usually used to call up saved preset locations or pre-defined patrols.

Custom Command

Leaving the "Button name" field empty means the command button will not be displayed in the homepage.

	Button name	Command
Command 1:	Tour 1	FF01000900010B
Command 2:		
Command 3:		
Command 4:		
Command 5:		

Save Close

You can use this function to create your own command buttons for operating and setting the connected PTZ device in the live picture of the video server.
The specific button function is described using a hexadecimal code (depending on the applicable PTZ protocol).
All ABUS speed-dome cameras use the PELCO D/P protocol.
Up to 5 user-defined buttons can be created.
Enter the desired name of the button (e.g. Tour 1) under “Button name”.

If you entered “Custom camera” as the camera protocol, you must define basic functions such as “up”, “down”, “left” and “right” as custom commands. Refer to the manual for the PTZ device for the applicable codes.

If you do not specify a button name, the button will not appear in the live picture.

The Pelco D/P protocol functions only with hexadecimal numbers.

Enter the HEX code for the desired function under "Command"
(e.g.: FF 01 00 09 00 01 0B**).**

The code must not include any spaces or special characters.
FF 01 00 09 00 01 0B → FF01000900010B

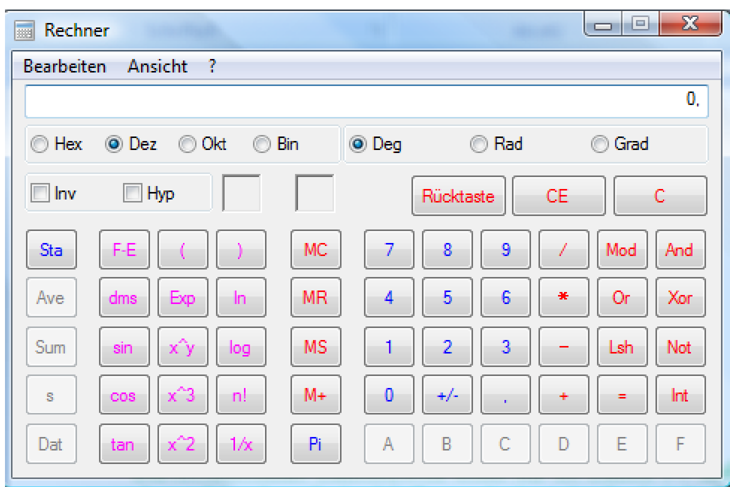
Preface to hexadecimal numbers

In the following chapter, a number of examples are used to explain the hexadecimal number system.

Decimal	Hex	Decimal	Hex	Decimal	Hex
1	1	11	B	30	1E
2	2	12	C	40	28
3	3	13	D	50	32
4	4	14	E	60	3C
5	5	15	F	70	46
6	6	16	10	80	50
7	7	17	11	90	5A
8	8	18	12	100	64
9	9	19	13	500	1F4
10	A	20	14	1000	3E8

The hexadecimal number system is based on numbers from 0-9 and letters from A-F. Note that the hexadecimals are added for the calculation of checksums.

An useful aid for converting decimal into hexadecimal numbers and adding hexadecimals is the Microsoft Windows calculator, which should be set to “Scientific” mode.



Dome control commands for TV7600, TV6702, TV7604 (Pelco)

Command structure

Word 1	Word 2	Word 3	Word 4	Word 5	Word 6	Word 7
Synch byte (always FF)	Address (ID of the analogue camera)	Command 1	Command 2	Data 1	Data 2	Checksum word 2-6

Checksum calculation:

Word 7= word 2 + word 3 + word 4 + word 5 + word 6

Word explanation:

"Word1" is always "FF"
"Word2" is the ID of the analogue camera
"Word3"–"Word4" define the different PTZ functions ("save preset", "start patrol" etc.)
"Word5"–"Word6" define e.g. the numbering of the preset locations and patrols.
If you wish to go to a preset location, you also have to define which preset location number is to be selected.
"Word7" is the sum of words 2-6, and is also referred to as the checksum

Example: "Go to preset location 1" has the command: FF 01 00 07 00 **01** 09

Word 1 is always FF
Word 2 is always the ID of the speed dome
Word 3 and word 4 define the function: "Go to preset location"
Words 5 and 6 define the preset location to which the video server should go.
Word 7 is the checksum

Explanation: In word 6, the hex number 01 stands for preset 1.
If you would then like to go to preset location 15, you would enter 0F for word 6.

Example: "Go to preset location 15" has the command: FF 01 00 07 00 **0F** 17
This procedure is the same when selecting patrols or other calculable function structures.

Do not forget to recalculate the checksum every time the command is changed.
In the above example, changing the command from preset 1 to preset 15 resulted in the checksum increasing by 14.

Overview of commands:

Command	Word 3	Word 4	Word 5	Word 6
Down	00	10	00	2A
Up	00	08	00	3C
Rotate Left	00	04	2E	00
Rotate Right	00	02	06	00
Stop	00	00	00	00
Menu	00	11	00	00
Start Patrol	00	00	09	01 to 08
Scan	00	0F	00	01
Zoom Out	00	20	00	01
Zoom Wide	00	40	00	01
Focus Near	01	00	00	01
Focus Far	00	80	00	00
Iris Close	04	00	00	00
Iris Open	02	00	00	00
Save Preset	00	03	00	01 to C8
Delete Preset	00	05	00	01 to C8
Go to Preset	00	07	00	01 to C8
Set Auxiliary	00	09	00	01 to 08
Clear Auxiliary	00	0B	00	01 to 08
Remote Reset	00	0F	00	00
Set Zone Start	00	11	00	01 to 08
Set Zone End	00	13	00	01 to 08
Write Char. To Screen	00	15	X Position 00 to 28	ASCII Value
Clear Screen	00	17	00	00
Alarm Acknowledge	00	19	00	Alarm No.
Zone Scan On	00	1B	00	00
Zone Scan Off	00	1D	00	00
Set Pattern Start	00	1F	00	00
Set Pattern Stop	00	21	00	00
Step Through Pattern	00	23	00	00
Set Zoom Speed	00	25	00	00 to 03
Set Focus Speed	00	27	00	00 to 03
Camera Default Setting	00	29	00	00
Auto Focus auto/on/off	00	2B	00	00-02
Auto Iris auto/on/off	00	2D	00	00-02
AGC auto/on/off	00	2F	00	00-02
BLC on/off	00	31	00	01-02
Auto White Balance on/off	00	33	00	01-02

13. Application

This allows you to automate tasks in the video server. The application configuration comprises 3 sections: event, server and medium. A typical application example may look like the following: due to motion detection (event), an email (server) with an alarm picture (medium) is sent to a user.

Event setup
Click **“Add”** to create a new event. Up to 3 events can be set.

"Event name" Assign a unique name to the event, under which the event configuration is to be saved
"Enable this event" Select this option to activate the programmed result.
"Priority" Events with higher priority are completed first
"Detect next event after" Time between events to be executed (e.g.: with motion detection)

Event Settings

Event name:
Enable this event
Priority: Normal
Detect next event after 10 second(s).
Note: This can only applied to motion detection and digital input

Trigger
Video motion detection
Periodically
Digital input
System boot
Recording notify
Camera tampering detection
Video loss
IP changed
Video restore

Event Schedule
Sun Mon Tue Wed Thu Fri Sat
Time
Always
From 00:00 to 24:00 [hh:mm]

Action
Trigger digital output for 1 seconds
Backup media if the network is disconnected
Move to preset location:
Note: Please configure Preset locations first
Add Server Add Media

Server	Media	
SD	-----None-----	SD Test View
NAS	Snapshot	Create folders automatically Customized folder %Y%M%D/%H View

13.1 Trigger settings

"Video motion detection" Activate the desired motion window.
"Periodically" The event is triggered periodically. Maximum setting is 999 minutes.
"Digital input" Triggered if a signal is present at the alarm input (e.g.: door contact).
"System boot" Event is triggered when the system is rebooted (after a power failure).
"Recording notify" If the destination storage (medium) is full or if a cyclic recording is overwritten, an alarm is triggered.
"Camera tampering detection" An alarm is triggered if the system detects that the connected analogue camera has been tampered with.

“Video loss” An alarm is triggered if the video signal is interrupted.
“IP changed” As long as a new IP address is assigned to the video server, an alarm is triggered.
“Video restore” Triggered when the video signal is restored following a malfunction.

Event schedule

“**Sun**” – “**Sat**” allows you to select the day of the week for executing an event.
“**Always**” Activates the event at all times (24 hours).
“**From**” – “**to**” The event times are restricted.

13.2 Server configuration

You can save up to 5 servers in the network camera. Click **“Add”** to configure a new server. The server of type **“SD”** is pre-configured and defines the SD card unit as the destination for saving data. You can configure the following server types:

- Email: enter the access data here
- FTP: enter the access data here. Address convention: ftp.abus-sc.com
- HTTP: enter the access data here. Address convention: http://abus-sc.com/cgi-bin/upload.cgi
- Network storage: Address convention: \\192.160.0.5\NAS

Server name:
Server Type
Email:
Sender email address:
Recipient email address:
Server address:
User name:
Password:
Server port 25
This server requires a secure connection (SSL)
FTP:
HTTP:
Network storage:
Test Save Close

Once you have entered the access data, save your settings. Before closing the window, it is advisable to execute a **“Test”**. The result is displayed in a new window of the browser.

13.3 Media settings

You can save up to 5 media settings in the video server.

Media name: test

Media Type

Snapshot

Source: Stream1

Send 1 pre-event image(s) [0~7]

Send 1 post-event image(s) [0~7]

File name prefix:

Add date and time suffix to file name

Video Clip

System log

Custom Message

Save Close

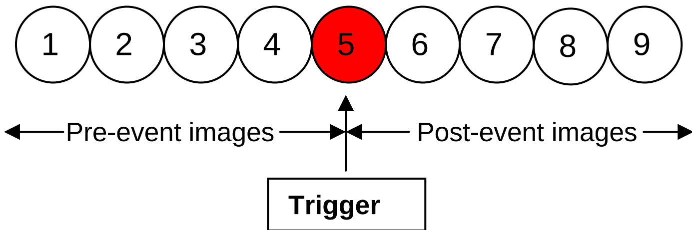
"**Media name**" Unique name for the medium.

There are 4 different media types:
- Snapshot (JPEG file)
- Video clip (MP4 format)
- System log (TXT log)
- Custom message (TXT format)

Each medium that you create can only be linked with one event.
Assigning a medium twice results in the incorrect functioning of the video server.
If you wish to use the same media type for two events, you must create two separate media types beforehand.

Snapshot

"**Source**" The recording can be made from video streams 1–4.
"**Send pre-event image(s)**" Number of snapshots before an event.
"**Send post-event image(s)**" Number of snapshots after an event.



“**File name prefix**” Enter a name that will prefix the snapshot file name.
“**Add date and time suffix to file name**” Adds the date and time to the snapshot so that you can more easily distinguish between the file names of snapshots either in sequential or event-controlled operation. Example: “video@20030102_030405.jpg” means that the JPEG picture was taken on January 2, 2003 at 03:04:05 (i.e., just after 3:04 am). If you omit this suffix, the file is updated with the name “video.jpg” on the external FTP server according to the specified time interval.

The data name is structured as follows:
Prefix_YYYYMMDD_HHMMSS : ABUS_20091115_164501

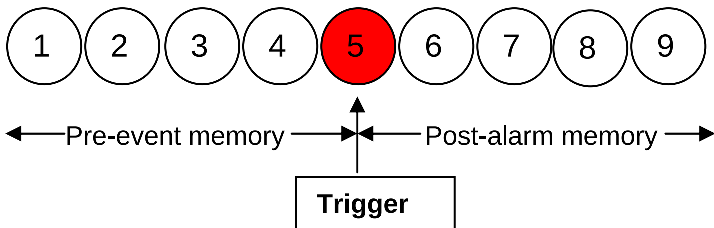
- Prefix: see file name prefix
- Y: placeholder for year, YYYY = 2009
- M: placeholder for month, MM = 11
- D: placeholder for day, DD = 15
- H: placeholder for hours, HH = 16
- M: placeholder for minutes, MM = 45
- S: placeholder for seconds, SS = 01

Video clip

“**Source**” The recording can be made from video streams 1-4.

The video stream that is configured in “Audio and Video” under “Select caching stream” is offered as a source.

“Pre-event recording” Pre-event recording interval in seconds (max. 9 seconds).
“Maximum duration” Maximum duration for each file (max. 10 seconds).



“Maximum file size” Maximum size of the file in kByte (max. 800 kByte).
“**File name prefix**” Enter a name that will prefix the video recording file name.
(see snapshot section for details)

Log file
Saves the current system log contents in a text file.

Custom Message
A user-defined message in the form of a text file is sent additionally.

13.4 Action

Action

Trigger digital output for 1 seconds

Backup media if the network is disconnected

Move to preset location:

Note: Please configure Preset locations first

Add Server | Add Media

	Server	Media	
	SD	-----None-----	SD Test View
	NAS	Snapshot	Create folders automatically
			Customized folder %Y%M%D/%H
			View

Here, you can configure the action that is to be executed if an alarm has been triggered.
"Trigger digital output for" When this option is enabled, the relay output for the video server is activated.
"Move to preset location" A preset location is activated when the alarm is triggered.
"Server" the selected medium is sent on a particular server (e.g. an email is sent with a snapshot).

"Create folders automatically" Folders are automatically created in the directory of the network drives

"Customized folder" The unique name of the folder is determined using variables.
The variables that are available can be found in the table below.

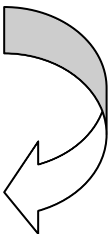
Symbol	Example/function
/	*Create a new folder*
%IP = IP address	*192.168.0.1*
%N = Event name	*Motion_W1*
%Y = Year	*2010*
%M = Month	*03*
%D = Day	*04*
%H = Hour	*14*
"Example text"	*"Example text"*

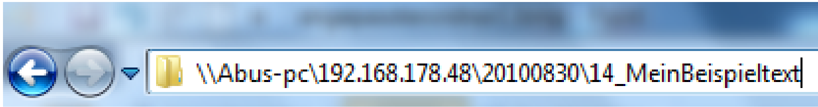
Example:
The following entry would generate this path.

Create folders automatically

Customized folder %IP/%Y%M%D/%H_MeinBeispieltext

View





13.5 Application overview

Here, you can view all the “Events”, “Media types” and “Servers” that are configured in the video server. You can check, delete and add the different settings here.
You can also check the different parameters such as name, status, trigger, address.

Event Settings

Name	Status	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Time	Trigger
ABUS	ON	V	V	V	V	V	V	V	00:00~24:00	boot

Add | ABUS | Delete | Help

Server Settings

Name	Type	Address/Location
NAS	ns	\\my_nas\disk\folder

Add | Delete

Media Settings

Available memory space: 9550KB

Name	Type
Snapshot	snapshot

Add | Delete

14. Recording

The recording section allows you to set up recordings with the option of setting up permanent video recordings for SD cards or network shares. You can save up to 2 video settings in the video server.
Click **“Add”** to create a new recording.

Recording name:

Enable this recording

Priority: Normal

Source: Stream1

Trigger

Schedule

Network fail

Recording Schedule

Sun Mon Tue Wed Thu Fri Sat

Time

Always

From 00:00 to 24:00 [hh:mm]

Destination SD

Note: To enable recording notification please configure Application first

Save | Close

Destination: **“Network drive”**

Capacity:

- (•) Entire free space
- ( ) Reserved space: 15 Mbytes

File name prefix:

[ ] Create folders automatically

Customized folder : %Y%M%D/%H

[ ] Enable cyclic recording

Note: To enable recording notification please configure Application first

Save Close

“**Recording name**” A unique name for a recording entry.
“**Enable this recording**” Select this option to activate the recording entry.
“**Priority**” Recordings with a higher priority are executed first.
“**Source**” The recording can be made from video streams 1-4.
“**Schedule**” The recording schedule is used.
“**Network fail**” If a network error occurs, the data is automatically saved onto SD card.
“**Sun**” – “**Sat**” allows you to select the day of the week for a recording.
“**Always**“ Activates the recording at all times.
“**From**“ – “**to**” The recording times are restricted.
“**Destination**” SD card or network folder.
“**Entire free space**” The maximum amount of space on the destination storage medium is used.
“**Reserved space**” Defines how many MB of free memory space should be reserved.
“**Enable cyclic recording**” Activates the cyclic recording function. If the set value is reached during the data recording, the oldest data is overwritten.

For more detailed information about “Create folders automatically”, refer to section “13.4 Action”.

If the “Customized folder” option is enabled, the cyclic recording function cannot be used.

Recording overview

“Name (video)” Opens the recording configuration page.
“Status (ON)” Sets the recording status to ON or OFF.
“Destination (SD)” Opens a file list with the saved recordings.

Recording Settings

Name	Status	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Time	Source	Destination
ABUS	ON	V	V	V	V	V	V	V	00:00~24:00	stream1	SD

Add SD Test ABUS Delete

15. Local memory

This section explains how you can manage the local memory (SD card) of the video server. Cards of type SD/SDHC Class 6 of up to 32 GByte are supported.

SD card management

SD card management

SD card status: Ready

Total size:	31830832 KBytes	Free size:	29837312 KBytes
Used size:	1993520 KBytes	Use (%):	6.263 %

Format

SD card control:

Enable cyclic storage

Enable automatic disk cleanup

Maximum duration for keeping files: 7 days

Save

Use the **"Format"** function if you are using the card in the video server for the first time.

Select the **"Enable cyclic storage"** option if the oldest data should be overwritten when the storage capacity of the SD card is full.

If you select **"Enable automatic disk cleanup",** the contents of the SD card are deleted after the maximum duration for keeping files is reached.

Searching and viewing the records

If no criteria are selected, the list of results will always include all recordings.

Searching and viewing the records

File attributes:

Trigger type:	Digital input	Video loss	Video restore
	System boot	Recording notify	Motion
	Periodically	Network fail	IP changed
	Tampering		
Media Type:	Video Clip	Snapshot	Text
Locked:	Locked	Unlocked	

Trigger time:

From:	Date		Time	
to:	Date		Time	
		(yyyy-mm-dd)		(hh:mm:ss)

Search

"Trigger type" Select one or more characteristics which apply to a recording that was made on the SD card.
"Trigger time" Select the desired period.

Click "Search". All the recordings that meet your criteria are displayed in the list of results.

List of results

Number of entries on one page

Search results

Show 10 entries   Search: Search

	Trigger time	Media Type	Trigger type	Locked
☐	2000-01-15 15:02:24	Video Clip	Periodically	No
☐	2000-01-15 15:03:24	Video Clip	Periodically	No
☐	2000-01-15 15:04:24	Video Clip	Periodically	No
☐	2000-01-15 15:05:24	Video Clip	Periodically	No
☐	2000-01-15 15:06:23	Video Clip	Periodically	No
☐	2000-01-15 15:07:23	Video Clip	Periodically	No
☐	2000-01-15 15:08:23	Video Clip	Periodically	No
☐	2000-01-15 15:09:23	Video Clip	Periodically	No
☐	2000-01-15 15:10:24	Video Clip	Periodically	No
☐	2000-01-15 15:11:24	Video Clip	Periodically	No

Showing 1 to 10 of 857 entries   Scroll pages

View | Download | Uncheck All | JPEGs to AVI | Lock/Unlock | Remove

"View" Shows the selected recording in a new window.
"Download" Allows you to download the selected recording.
"JPEGs to AVI" You can select several JPEG single picture recordings (selection box) and convert these into an AVI file.
"Lock/Unlock" Individual recordings can be locked. Locked recordings will not be overwritten through cyclic storage. Press the button again (unlock) to remove this attribute.
"Remove" The selected recording is deleted.

You can also evaluate the data stored on the SD card using the SD card reader on your PC. The recorded data is displayed according to file type with the date and time in the file name.

16. Log file

Click this link on the configuration page to display the system log file. The contents of the file supply useful information about the configuration and the connection following a system start. The standard of the log file is RFC 3164. You can also send data to a log server. Enable "Remote Protocol" and enter the IP address and the port number of the server.

17. Parameter list

Click this link on the configuration page to display all system parameter sets. This information can be provided for support cases.

18. Management

Reboot
Setting for reboot camera
Note: When you choose duration mode, the camera will reboot at 24:00 after N day(s)
Reboot the device
Duration Mode :
Every 1 [1~30] Day(s)
Schedule Mode :
Sun Mon Tue Wed Thu Fri Sat
Time 00:00 [hh:mm]
Save Reboot Now

Save Reboot Now
Restore
Restore all settings to factory default except settings in
Network Type Daylight Saving Time
Restore
Export files
Export daylight saving time configuration file Export
Export setting backup file Export
Upload files
Update daylight saving time rules Durchsuchen... Upload
Upload setting backup file Durchsuchen... Upload
Upgrade firmware
Select firmware file Durchsuchen...
Upgrade

Reboot
Press the “Reboot Now” button to restart the video server. You can also configure an automated device reboot. This may be helpful if network problems occur. We recommend rebooting the video server on a weekly basis if you experience problems.

Restore
Click to restore the factory settings. All previous settings are discarded.

Export files
Press to export your video server settings into a file. You can also export and save the daylight saving time configuration file.

Upload files
Press “Browse...” and select the correct configuration file.
Then press “Upload” and wait until the settings have been restored.

Upgrade firmware
Like an update with the installation wizard, you can update the firmware of the video server here. You can download the latest firmware from www.abus-sc.com. Select the firmware file (*.pkg) and press “Upgrade”. The update takes a short time. When you restart the video server, it is started with the new firmware.

Never disconnect the video server from the power supply during an firmware upgrade, otherwise you risk causing irreparable damage.
A firmware upgrade can last up to 10 minutes.

19. Maintenance and Cleaning

19.1 Function Test

Regularly check the technical safety of the product, e.g. check the housing for damage.

If safe operation is no longer possible, cease operating the product and safeguard it against accidental operation.

Safe operation is no longer possible if:

- the device shows visible damage,
- the device no longer functions, and
- the device has been stored in adverse conditions for a long period of time, or
- the device has been subject to stress during transportation.

This product is maintenance-free for you. There are no components to service or anything inside the product to check. Never open it.

19.2 Cleaning

Clean the device with a clean, dry cloth. The cloth can be dampened with lukewarm water if it gets dirty.

Make sure that liquid does not get into the inside of the device as this will cause damage.
Do not use any chemical cleaning products as this could damage the surface of the housing.

20. Disposal

Devices that have been marked accordingly may not be disposed of as domestic waste. At the end of its service life, dispose of the product according to the applicable legal requirements.
Please contact your dealer or dispose of the products at the local collection point for electronic waste.

21. Technical data

Model number	TVIP40000
Camera type	Videoserver
Resolution	QCIF, CIF, 4CIF, D1 176 x 144 – 720 x 576 (intermediate levels can be freely selected)
Pixels (total)	720x576
Pixels (effective)	720x576
Digital zoom	4 x
Image compression	H.264, MPEG-4, MJPEG
Frame rate	H.264 720X480@30FPS, 720x576@25FPS
	MPEG-4 720X480@30FPS, 720x576@25FPS
	MJPEG 720X480@30FPS, 720x576@25FPS
Video norm	PAL, NTSC
Number of parallel streams	4
Number of maximum users	10
Motion detection	3 zones
Pre-alarm/post-alarm memory	Yes
Image overlay	Date, camera name, private zones
Alarm inputs (NO/NC)	1
Digital output	1 (12VDC@400mA)
Audio	Audio output (Speaker Out), audio input, 2-way audio
Alert message	E-mail / FTP / HTTP notification / relay output / NAS drive / SD card
Supported browsers	Mozilla Firefox or Internet Explorer 6.x and higher
Software supported	eytron VMS, ONVIF support
SD card	max. 32 GB (SD/SD-HC)
RS-485 port	Yes
PTZ protocols	Pelco D, Pelco P, LiLin, Samsung scc643, DynaDome / SmartDome
Network connection	RJ45 Ethernet 10/100 Base-T with PoE
Network protocols	IPv4, IPv6, TCP/IP, HTTP, UPnP, RTSP/RTP/RTCP, IGMP, SMTP, FTP, DHCP, NTP, DNS, CoS, QoS, SNMP, 802.1X
Encryption	HTTPS SSLv3
Access protection	IP address filter, user name, password, 3 authorisation levels
Power supply	12 VDC, 24 VAC, 802.3af PoE
Current consumption	Max. 5.0 Watt
Operating temperature	0 °C ~ 55 °C
Dimensions (W x H x D)	75 x 35 x 150 mm
Certification	CE, RoHS, C-Tick

22. URL Commands

For some customers who already have their own web site or web control application, the Network Camera/Video Server can be easily integrated through URL syntax. This section specifies the external HTTP-based application programming interface. Please refer to Appendix for complete URL command list.

23. License information

We point at the fact that the videoserver TVIP40000 among other things include Linux software source codes that are licensed under the GNU General Public Licence (GPL). To assure a GPL compliant usage of the used source codes we point at the licence terms of GPL.

Licence text

The licence text of the GNU General Public Licence can be found on the included software CD or on the ABUS Security-Center Homepage under http://www.abus-sc.de/DE/Service-Downloads/Software?q=GPL

Source Code

The used source codes are available on the ABUS Security-Center Homepage under
http://www.abus-sc.de/DE/Service-Downloads/Software?q=GPL
for free download.

Operation of the total system

With a download of the software packages (source codes) it is not possible to built a running total system. Therefore additional software applications and the network video server hardware is needed.

24. Technology license information

H.264, MPEG-4 AAC Technology

THIS PRODUCT IS LICENSED UNDER THE H.264, MPEG-4 AAC AUDIO PATENT LICENSE. THIS PRODUCT MAY NOT BE DECOMPILED, REVERSE-ENGINEERED OR COPIED, EXCEPT REGARD TO PC SOFTWARE, YOU MAY MAKE SINGLE COPIES FOR ARCHIVAL PURPOSES. FOR MORE INFORMATION, PLEASE REFER TO HTTP://WWW.VIALICENSING.COM.

H.264, MPEG-4 Visual Technology

THIS PRODUCT IS LICENSED UNDER THE H.264, MPEG-4 VISUAL PATENT PORTFOLIO LICENSE FOR THE PERSONAL AND NON-COMMERCIAL USE OF A CONSUMER FOR (i) ENCODING VIDEO IN COMPLIANCE WITH THE MPEG-4 VISUAL STANDARD ("MPEG-4 VIDEO") AND/OR (ii) DECODING MPEG-4 VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL AND NON-COMMERCIAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED BY MPEG LA TO PROVIDE MPEG-4 VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION INCLUDING THAT RELATING TO PROMOTIONAL, INTERNAL AND COMMERCIAL USES AND LICENSING MAY BE OBTAINED FROM MPEG LA, LLC. SEE HTTP://WWW.MPEGLA.COM.

AMR-NB Standard

THIS PRODUCT IS LICENSED UNDER THE AMR-NB STANDARD PATENT LICENSE AGREEMENT. WITH RESPECT TO THE USE OF THIS PRODUCT, THE FOLLOWING LICENSORS' PATENTS MAY APPLY:
TELEFONAKIEBOLAGET ERICSSON AB: US PAT. 6192335; 6275798; 6029125; 6424938; 6058359. NOKIA CORPORATION: US PAT. 5946651; 6199035. VOICEAGE CORPORATION: AT PAT. 0516621; BE PAT. 0516621; CA PAT. 2010830; CH PAT. 0516621; DE PAT. 0516621; DK PAT. 0516621; ES PAT. 0516621; FR PAT. 0516621; GB PAT. 0516621; GR PAT. 0516621; IT PAT. 0516621; LI PAT. 0516621; LU PAT. 0516621; NL PAT. 0516621; SE PAT 0516621; US PAT 5444816; AT PAT. 819303/AT E 198805T1; AU PAT. 697256; BE PAT. 819303; BR PAT. 9604838-7; CA PAT. 2216315; CH PAT. 819303; CN PAT. ZL96193827.7; DE PAT. 819303/DE69611607T2; DK PAT. 819303; ES PAT. 819303; EP PAT. 819303; FR PAT. 819303; GB PAT. 819303; IT PAT. 819303; JP PAT. APP. 8-529817; NL PAT. 819303; SE PAT. 819303; US PAT. 5664053. THE LIST MAY BE UPDATED FROM TIME TO TIME BY LICENSORS AND A CURRENT VERSION OF WHICH IS AVAILABLE ON LICENSOR'S WEBSITE AT HTTP://WWW.VOICEAGE.COM

ABUS
Security Tech Germany

eyseo.ip

TVIP40000

Manuel utilisateur

Version 10/2010

Mode d'emploi original. À conserver à porter de main.

Introduction

Cher Client,

Nous vous remercions d'avoir acheté ce produit.

Ce produit satisfait aux exigences de la législation nationale et des directives européennes applicables. Les avis, déclarations et documents correspondants peuvent être obtenus auprès du fabricant.
(www.abus-sc.com)

Pour maintenir cet état et garantir un fonctionnement sans risques, il est indispensable d'observer les règles et instructions de fonctionnement de ce mode d'emploi.

Avant toute mise en route, nous vous conseillons de lire attentivement l'intégralité de ce mode d'emploi en prêtant une attention particulière aux instructions d'utilisation et aux consignes de sécurité.

Tous les noms de sociétés et de produits mentionnés dans le présent document sont des marques déposées.

Pour toute question, veuillez contactez votre installateur ou votre revendeur !

Avis de non-responsabilité

Ce mode d'emploi a été rédigé avec le plus grand soin. Si vous deviez cependant y relever des omissions ou des inexactitudes, nous vous prions de bien vouloir nous en aviser à l'adresse indiquée au dos de ce mode d'emploi.
ABUS Security-Center GmbH décline toute responsabilité pour toute erreur technique ou typographique, et se réserve le droit d'apporter à tout moment des modifications au produit ou à son mode d'emploi sans avis préalable.
La société ne sera pas tenue responsable de quelconques dommages consécutifs directs ou indirects qui seraient liés au matériel, au fonctionnement ou à l'utilisation de ce produit.
Elle n'assume aucune garantie quant au contenu du présent document.

Explication des pictogrammes

Un éclair dans un triangle indique un risque pour la santé, par exemple un choc électrique.

Un point d'exclamation dans un triangle signale une remarque importante dont il convient de tenir compte.

Le symbole « i » dans un triangle signale des conseils et des informations utiles sur le fonctionnement du produit.

Conseils de sécurité importants

Tout dommage dû à la non-observation des instructions du présent mode d'emploi annule la garantie. ABUS ne sera tenue en aucun cas responsable de quelconques pertes indirectes !

ABUS décline toute responsabilité en cas de dommages matériels ou corporels qui seraient dus à la manipulation incorrecte du produit, ou au non-respect des consignes de sécurité indiquées.
En outre, toute utilisation impropre ou non-respect des consignes annule la garantie.

Cher Client,
Les consignes de sécurité suivantes sont destinées à protéger à la fois votre santé et l'appareil.
Veuillez lire attentivement les points ci-dessous :

- Aucune pièce interne de ce produit ne doit faire l'objet d'un entretien ou d'une réparation. Toute ouverture et tout démontage de ce produit entraînent l'invalidation de son homologation (CE) et de sa garantie.
- Toute chute, même de faible hauteur, risque d'endommager ce produit.
- Cet appareil peut être utilisé à l'intérieur.
- Veuillez suivre les instructions d'installation indiquées dans le chapitre correspondant du présent mode d'emploi.

Évitez d'utiliser cet appareil dans les conditions d'environnement défavorables suivantes :

- Humidité atmosphérique excessive
- Températures extrêmes
- Rayons directs du soleil
- Présence de poussières ou de gaz, vapeurs ou solvants inflammables
- Vibrations fortes
- Champs magnétiques puissants (tels que ceux rencontrés à proximité de machines ou de haut-parleurs)
- Installation sur une surface instable

Consignes de sécurité générales :

- Ne laissez pas traîner le matériel de conditionnement après déballage. Les sachets, sacs et feuilles en plastique ainsi que les pièces en polystyrène, notamment, peuvent être dangereux s'ils sont utilisés comme jouets par des enfants.
- Ne laissez pas un enfant prendre la serveur vidéo, il pourrait ingérer les petites pièces qui la composent.
- Veillez à n'introduire aucun objet à travers les orifices de l'appareil.
- Utilisez uniquement des accessoires spécifiés par le fabricant.
  Ne branchez jamais de pièces incompatibles sur l'appareil.
- Observez attentivement les consignes de sécurité et les modes d'emploi de tout autre appareil connecté.
- Vérifiez l'appareil avant l'installation afin de vous assurer qu'il ne présente aucun dommage. En cas de dommage, ne l'utilisez pas.
- Respectez les limitations concernant les tensions de fonctionnement présentées dans les caractéristiques techniques. La présence d'une haute tension peut détruire l'appareil et présenter un risque pour la santé (choc électrique).

Conseils de sécurité

1. Alimentation secteur : alimentation électrique 110 - 250 V c.a., 50/60 Hz / 12 V c.c., 1,5 A (fournie dans l'emballage)
   Vous ne devez utiliser ce produit qu'avec le type d'alimentation électrique indiqué sur la plaquette. Si vous ne connaissez pas avec certitude le type d'alimentation électrique dont vous disposez, adressez-vous à votre fournisseur d'électricité. Débranchez le produit du secteur avant toute opération d'entretien ou d'installation.

2. Surcharge
   Ne surchargez pas la prise murale, la rallonge ou l'adaptateur, vous pourriez provoquer un incendie ou un choc électrique.

3. Nettoyage
   Débranchez le produit de la prise secteur avant tout nettoyage. Pour dépoussiérer le produit, utilisez un tissu légèrement humide (sans solvant).

Avertissements

Observez toutes les consignes de sécurité et tous les conseils d'utilisation avant de mettre en marche l'appareil !

1. Pour éviter d'endommager le cordon ou la fiche d'alimentation, suivez les instructions suivantes :
   - Ne modifiez pas le cordon ou la fiche d'alimentation, et ne leur réservez pas un usage impropre.
   - Veillez à ne pas plier ni tordre le cordon d'alimentation.
   - Veillez à débrancher le cordon d'alimentation par la fiche.
   - Éloignez toute source de chaleur du cordon d'alimentation, afin d'éviter que son revêtement isolant ne fonde.

2. Pour éviter tout choc électrique, suivez les instructions suivantes :
   - N'ouvrez jamais le corps de l'appareil, sauf pour installer le disque dur.
     Débranchez toujours le produit du secteur avant toute intervention.
   - N'introduisez jamais d'objets métalliques ou inflammables dans le produit.
   - Installez un appareil de protection contre les surtensions pour éviter tout dommage de cet ordre.

3. N'utilisez pas le produit s'il ne fonctionne pas correctement. Toute utilisation continue d'un produit défectueux peut l'endommager gravement. Si le produit ne fonctionne plus ou plus convenablement, contactez votre distributeur.

Si vous installez cet appareil au sein d'un système de surveillance vidéo existant, assurez-vous que tous les appareils soient débranchés de tout circuit électrique, basse ou haute tension.

En cas de doute, faites appel à un électricien professionnel pour monter, installer et câbler votre appareil. Un raccordement électrique non conforme au réseau constitue un danger non seulement pour vous, mais aussi pour d'autres personnes.
Câblez l'installation en veillant à garder séparés les circuits à basse et à haute tension, et en vous assurant que ces circuits ne peuvent pas s'interconnecter dans des conditions d'utilisation normales ou en cas de dysfonctionnement.

Déballage

Veillez à déballer l'appareil en le manipulant avec le plus grand soin.

Si l'emballage original est endommagé d'une quelconque façon, vérifiez immédiatement l'appareil.
Si l'appareil présente des dommages, contactez votre revendeur.

Inhaltsverzeichnis

Usage

Une description détaillée des fonctions se trouve dans le chapitre « 4. Première mise en route ».

Toute autre utilisation que celle décrite ci-dessus peut endommager le produit et être à l'origine d'autres risques. En particulier, ce produit ne doit pas être utilisé dans le cadre d'autres applications, sous peine d'annulation de la garantie et de rejet de toute responsabilité liée. Ce principe vaut également en cas de modification non autorisée du produit.

Veuillez lire le mode d'emploi dans son intégralité avant toute mise en oeuvre de ce produit. Le mode d'emploi contient des instructions importantes pour un montage et une utilisation appropriés.

1. Éléments fournis

D1 Réseau serveur vidéo
TVIP40000

Alimentation électrique

Supports

Guide rapide

CD des logiciels
et du mode d'emploi

2. Installation

Assurez-vous que tous les accessoires repris ci-dessus sont bien fournis. Pour faire fonctionner la serveur vidéo , vous avez besoin d'un câble réseau Ethernet. Ce câble doit répondre aux spécifications UTP Cat 5 et ne doit pas présenter une longueur supérieure à 100 mètres.

2.1 Alimentation électrique

Avant de mettre en route l'installation, assurez-vous que la tension du secteur et la tension nominale de la serveur vidéo correspondent.

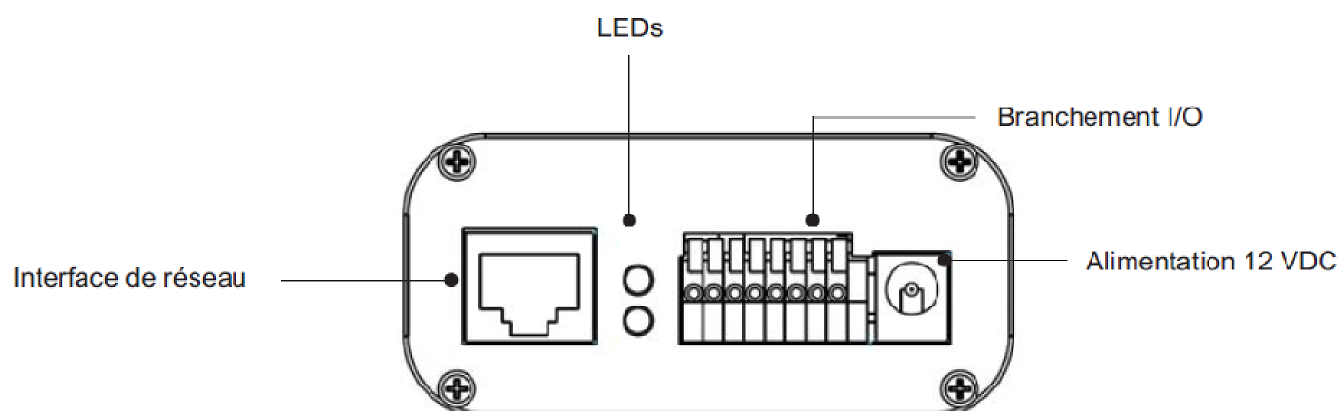
2.2 Installation de la serveur vidéo

Les étriers de retenue et les vis nécessaires au montage au mur du serveur vidéo sont compris dans la livraison.

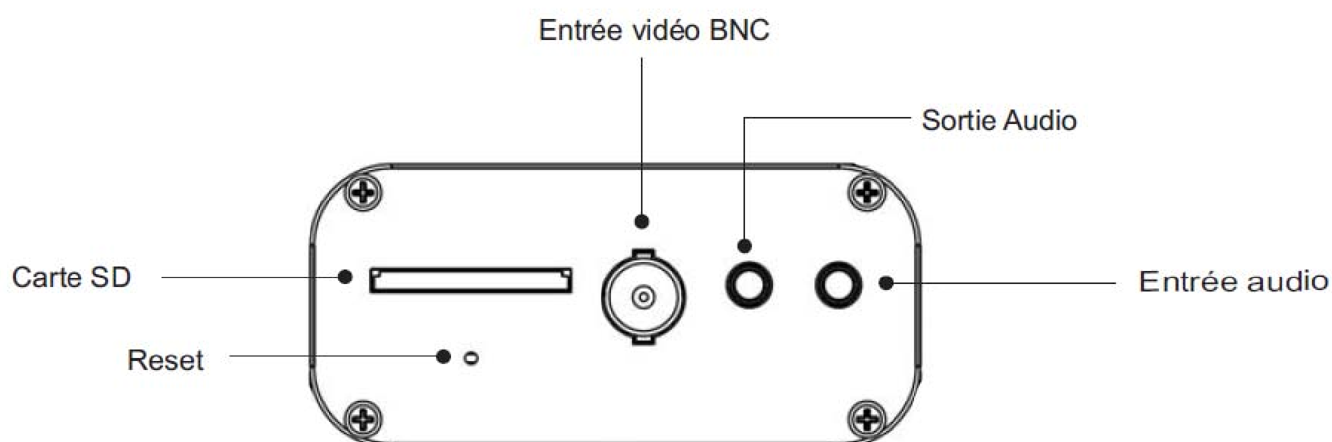
ATTENTION !
Veillez à débrancher la serveur vidéo de l'alimentation électrique avant de l'installer.

3. Description de la serveur vidéo

3.1 Vue de face

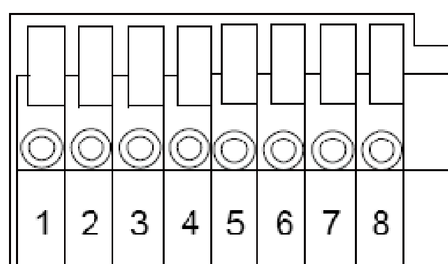


3.2 Vue de dos

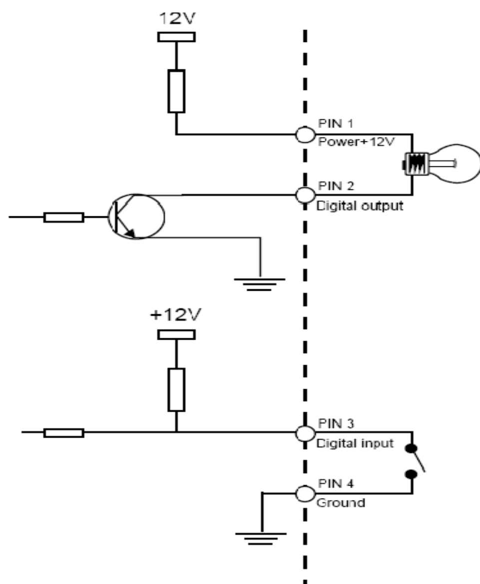


3.3 Entrée d'alarme et sorties numériques

Broche	Description
1	Sortie +12 V
2	Sortie numérique
3	Entrée numérique
4	Terre
5	Entrée 24V AC
6	Entrée 24V AC
7	RS-485 +
8	RS-485 -



3.4 Entrée-sortie de porte logique et affichage d'état



Description des DEL d'état :

État / couleur de la DEL	Vert	Rouge
Mise en marche du système	Éteinte	Allumée
Serveur vidéo éteinte	Éteinte	Éteinte
Recherche OK	1/s	Allumée
Problème réseau	Éteinte	Allumée
Mise à jour du microprogramme	1/s	0,1/s
Rétablissement des réglages d'usine	0,1/s	0,1/s

Pour **réamorcer** la serveur vidéo ou rétablir ses réglages d'usine, actionnez le bouton de réinitialisation à l'aide d'une pointe appropriée.

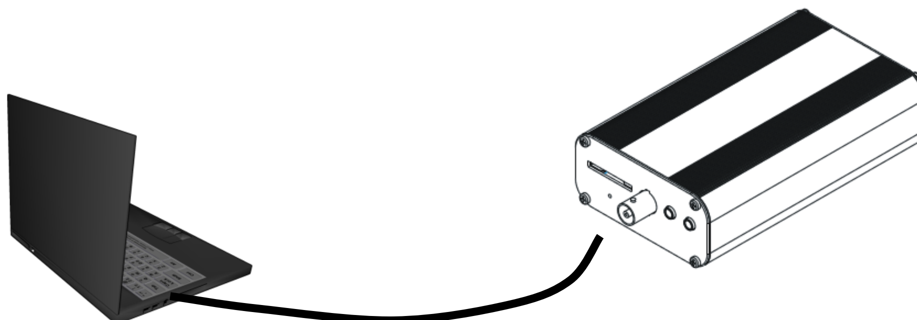
Redémarrage de la serveur vidéo : Exercez une seule pression sur le bouton de réinitialisation et attendez que la serveur vidéo redémarre.

Rétablissement des réglages d'usine : Pressez et maintenez le bouton de réinitialisation enfoncé pendant environ 30 secondes, jusqu'à ce que les DEL d'état commencent à clignoter. Tous les réglages seront réinitialisés pour rétablir les réglages d'usine.

4. Première mise en route

Connexion directe entre la serveur vidéo et un ordinateur de bureau ou portable

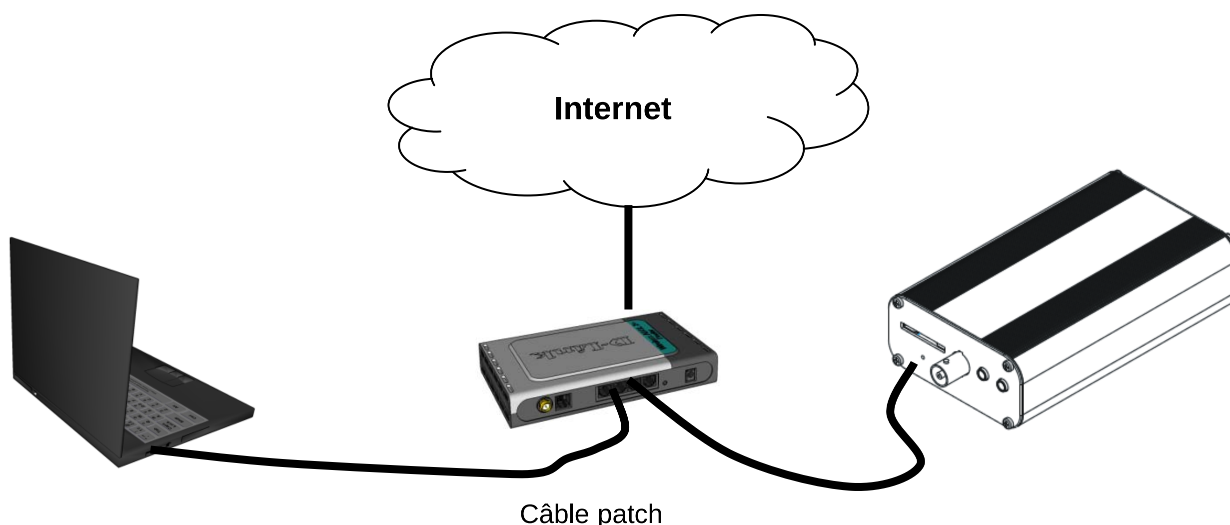
1. Procurez-vous un câble réseau croisé.
2. Raccordez le câble au port Ethernet de l'ordinateur et à la serveur vidéo réseau.
3. Branchez le bloc d'alimentation sur la serveur vidéo réseau.
4. Configurez sur l'ordinateur l'adresse IP 169.254.0.1.
5. Continuez au point 5.1 pour terminer cette procédure d'installation initiale et établir la connexion avec la serveur vidéo.



➀ Câble Ethernet croisé

Connexion de la serveur vidéo à l'aide d'un routeur ou d'un commutateur

1. Procurez-vous deux câbles de raccordement.
2. Raccordez le câble au port Ethernet de l'ordinateur et au routeur / commutateur.
3. Raccordez le câble réseau de la serveur vidéo au routeur / commutateur.
4. Branchez le bloc d'alimentation sur la serveur vidéo réseau.
5. Si votre réseau dispose d'un serveur DHCP, définissez les paramètres IP de l'ordinateur de telle sorte que celui-ci reçoive automatiquement une adresse IP.
   S'il n'y a pas de serveur DHCP, donnez à l'ordinateur l'adresse IP 169.254.0.1.
6. Continuez au point 5.1 pour terminer cette procédure d'installation initiale et établir la connexion avec la serveur vidéo.



Câble patch

4.1 Premier accès à la serveur vidéo réseau

Le premier accès à la serveur vidéo réseau s'effectue par le biais de l'assistant d'installation « Installation Wizard 2 ».
Une fois lancé, l'assistant recherche automatiquement tous les serveurs vidéo et toutes les serveur vidéo s réseau EyseoIP connectés.

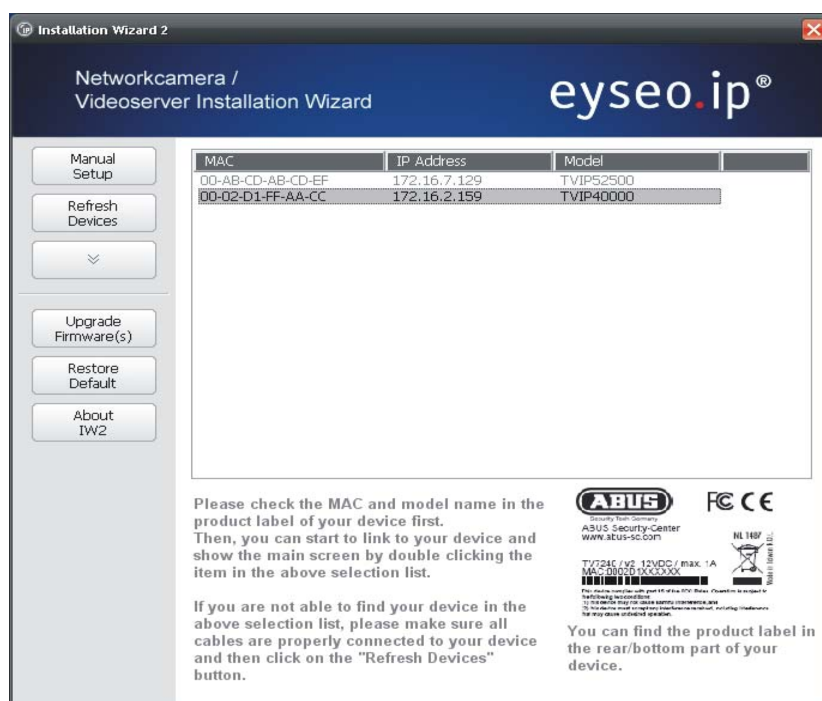
Le programme de cet assistant se trouve sur le CD dans le répertoire **CD-ROM\Tools\EyseoIP Tools\.**

Installez le programme sur l'ordinateur et lancez-le. L'assistant recherche automatique les serveur vidéo s réseau EyseoIP sur le réseau.

L'adresse IP réglée par défaut à l'usine est **169.254.0.99**. Si vous n'utilisez pas l'assistant d'installation, vous ne pourrez établir une connexion avec la serveur vidéo que si l'adresse IP de l'ordinateur est comprise entre 169.254.0.1 et 169.254.0.98.

Si le réseau comprend un serveur DHCP, l'adresse IP de l'ordinateur et de la serveur vidéo réseau sera définie automatiquement.

Lancez à présent l'assistant d'installation. S'il n'y a pas de serveur DHCP, l'assistant d'installation ajoute une adresse IP virtuelle dans la plage 169.1254.0.xx. Tant que l'assistant d'installation est actif, vous pouvez accéder à la serveur vidéo réseau en utilisant cette adresse IP virtuelle. Nous vous recommandons d'adapter immédiatement les paramètres réseau de la serveur vidéo aux paramètres IP du réseau de l'ordinateur.



Une fois l'assistant d'installation fermé, cette adresse IP virtuelle supplémentaire est supprimée. Si l'adresse IP de la serveur vidéo IP correspond à ce moment encore à une plage d'adresses IP différente de celle de l'ordinateur, il n'est plus possible d'accéder à la serveur vidéo IP.

4.2 Connexion à la serveur vidéo réseau à l'aide d'un navigateur web

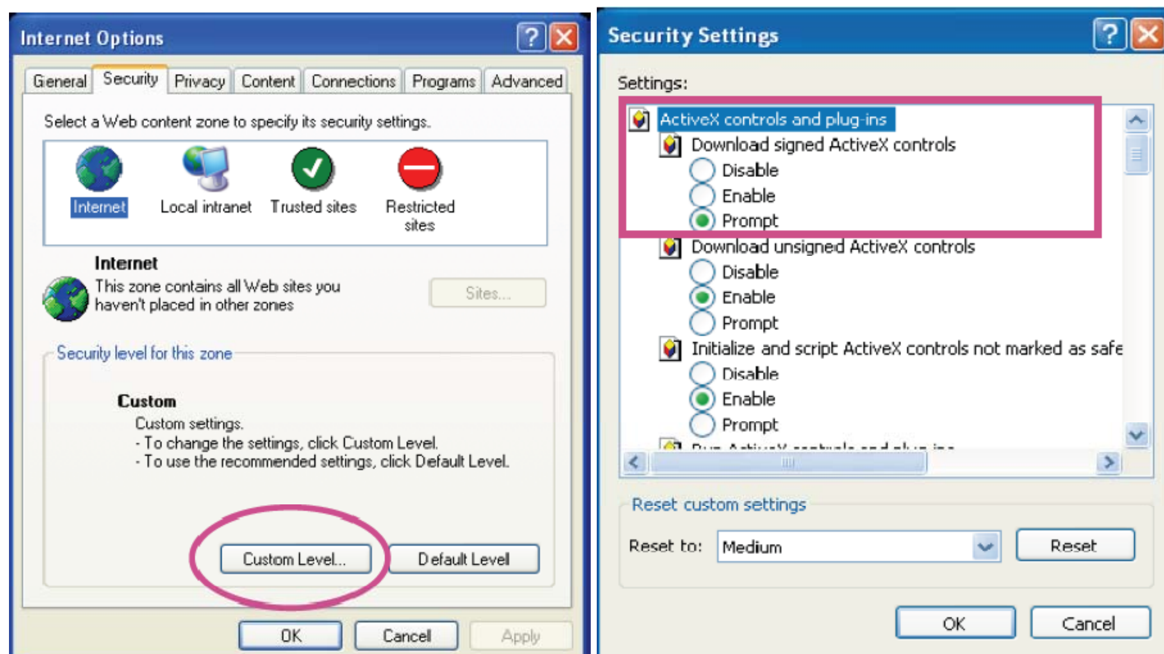
Si vous vous connectez à la serveur vidéo réseau avec Mozilla Firefox ou Netscape, un flux QuickTime apparaît. Pour cela, il faut que le programme Apple QuickTime soit installé.

Pour afficher le flux vidéo avec Microsoft Internet Explorer, vous avez besoin d'un module d'extension vidéo. Ce module est installé lors de la connexion à la serveur vidéo réseau. Une fenêtre vous invite alors à installer le module d'extension. Cliquez sur le bouton « Installer » pour continuer et installer ce programme. Si l'installation est bloquée en raison des paramètres de sécurité d'Internet Explorer, vous devrez modifier ces paramètres pour pouvoir continuer.

4.3 Installation du module d'extension ActiveX

Si vous utilisez Mozilla Firefox ou Netscape, votre navigateur doit faire appel à QuickTime pour retransmettre le fluxvidéo en direct. Si vous n'en disposez pas encore sur votre ordinateur, téléchargez QuickTime, puis ouvrez
votre navigateur web.

4.4 Réglage des paramètres de sécurité



REMARQUE IMPORTANTE
Les paramètres de sécurité d'Internet Explorer peuvent empêcher l'affichage du flux vidéo. Si c'est le cas, vous devez choisir un niveau de sécurité inférieur dans « Options Internet / Sécurité » et activer les contrôles ActiveX dans « Personnaliser le niveau ».

4.5 Authentification par mot de passe

Aucun mot de passe d'accès à la serveur vidéo n'est défini dans les réglages d'usine. Pour des raisons de sécurité, il est impératif que l'administrateur définisse un mot de passe une fois la configuration initiale terminée. Lorsqu'un mot de passe d'administrateur (admin) est défini, la serveur vidéo exige la saisie d'un nom d'utilisateur et d'un mot de passe à chaque accès.

Le nom d'utilisateur par défaut permanent pour l'administrateur est « **root** ». Il ne peut pas être modifié. Le seul moyen de réinitialiser le mot de passe, en cas d'oubli, est de réinitialiser la serveur vidéo pour rétablir les réglages d'usine.

Pour accéder à la serveur vidéo , saisissez le nom d'utilisateur « root » et le mot de passe que vous avez défini.

-> Lorsque l'authentification réussit, vous êtes connecté à la serveur vidéo et un flux vidéo s'affiche.

4.6 Connexion à la serveur vidéo réseau à l'aide d'un lecteur RTSP

Vous pouvez afficher les flux vidéo MPEG-4 en vous connectant à la serveur vidéo réseau à l'aide d'un lecteur de média compatible RTSP. Les lecteurs de média gratuits suivants prennent en charge cette norme RTSP :

- VLC Media Player
- Real Player
- QuickTime Media Player

L'adresse RTSP doit être saisie comme suit :

rtsp://<adresse IP de la serveur vidéo réseau>:<port rtsp>/<nom du flux vidéo>

La procédure de modification du nom du flux vidéo est décrite plus loin.

Exemple:
rtsp://192.168.0.99:554/live.sdp

4.7 Connexion à la serveur vidéo réseau à l'aide d'un téléphone mobile

Assurez-vous que votre téléphone mobile est capable d'établir une connexion internet. Le téléphone doit encore disposer d'un lecteur de média compatible RTSP tel que :

- Real Player
- Core Player

Pour plus d'informations, reportez-vous au chapitre « Transmission RTSP ».

Il est à noter que l'accès peut être limité en raison de la bande passante du réseau mobile. Pour optimiser le flux vidéo, nous vous recommandons les paramètres suivants :

Compression vidéo	MPEG-4
Résolution	176x144
Image I	1 seconde
Qualité vidéo (débit binaire constant)	40 Kbit/s
Compression audio (GSM-AMR)	12,2 Kbit/s

Si le lecteur de média ne prend pas en charge l'authentification RTSP, il convient de désactiver cette option dans les paramètres RTSP de la serveur vidéo réseau.

L'adresse RTSP doit être saisie comme suit :

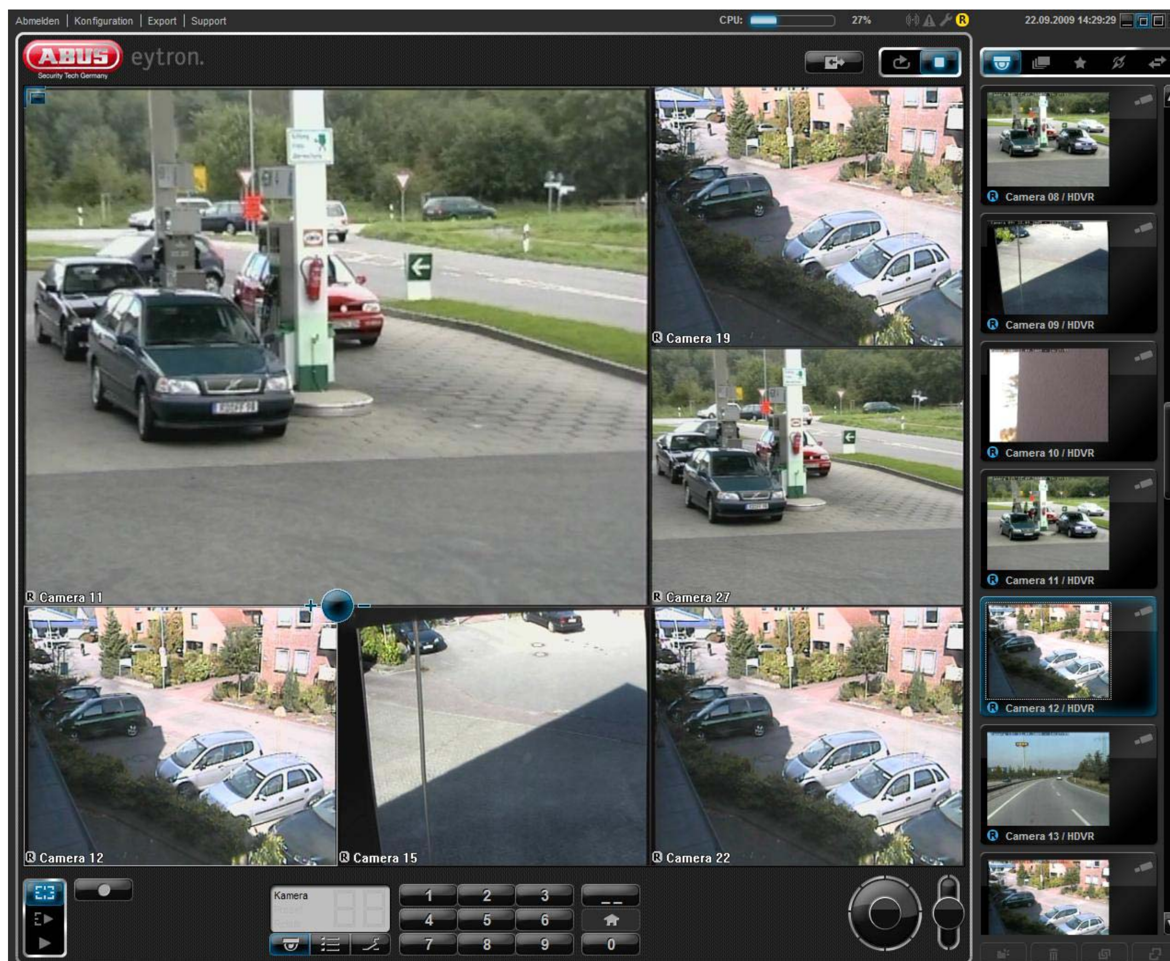
rtsp://<adresse IP de la serveur vidéo réseau>:<port rtsp>/<nom du flux vidéo>

La procédure de modification du nom du flux vidéo est décrite plus loin.

Exemple:
rtsp://192.168.0.99:554/live.sdp

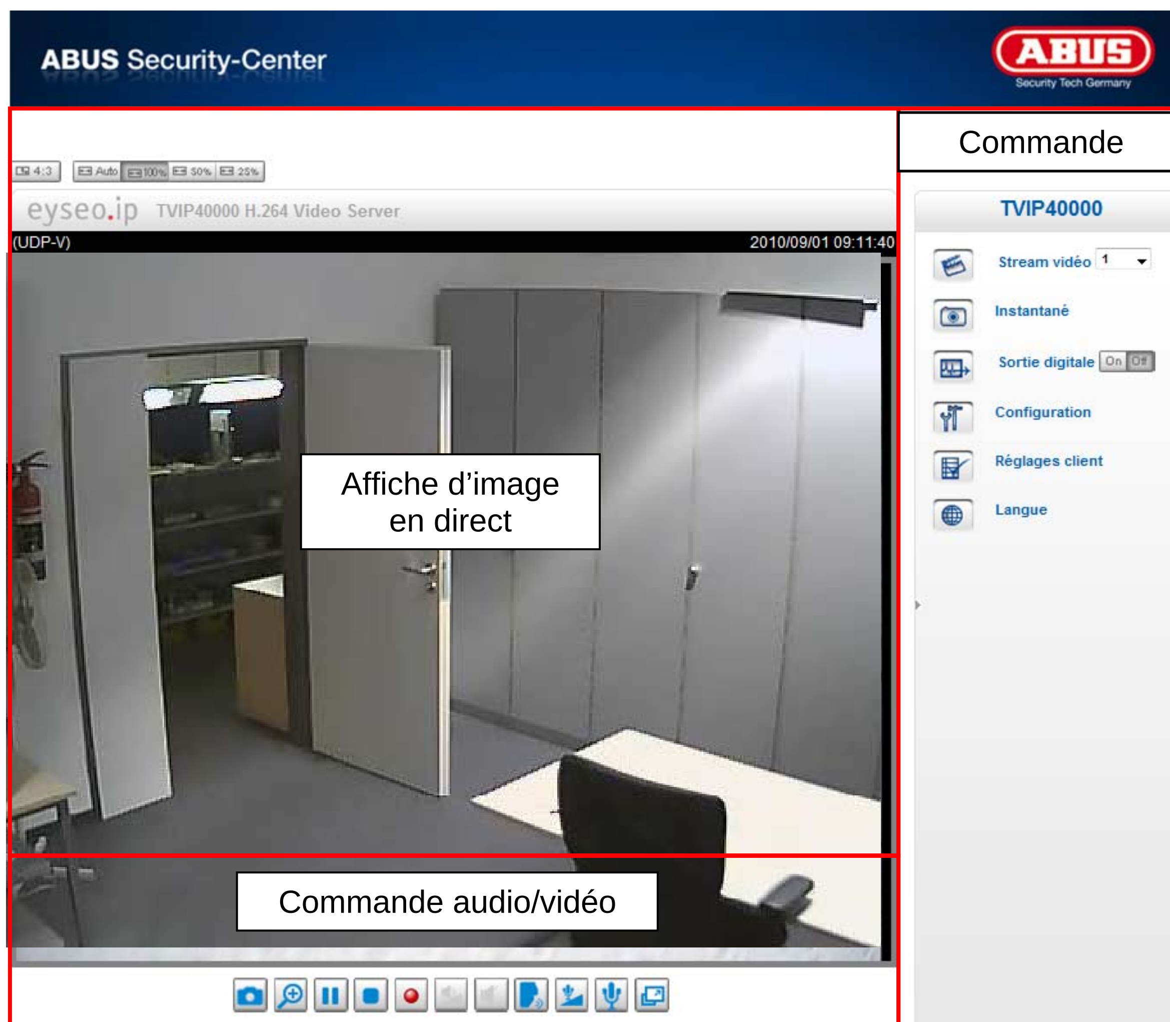
4.8 Connexion à la serveur vidéo réseau à l'aide d'eytron VMS Express

Le CD fourni contient le logiciel d'enregistrement gratuit eytron VMS Express. Ce logiciel autorise la connexion à plusieurs serveur vidéo s IP ainsi que l'affichage et l'enregistrement des images qu'elles transmettent. Pour plus d'informations, reportez-vous au manuel du logiciel, sur le CD.



5. Fonctions d'utilisateur

Ouvrez la page initiale du serveur vidéo. La fenêtre est divisée en plusieurs zones principales :



Affiche d'image en direct

- Modification du niveau de zoom au moyen de la molette de la souris.
- Cliquez dans l'image en direct pour pouvoir commander directement la rotation ou l'inclinaison analogique de la caméra.

Commande du serveur vidéo

Flux vidéo

Sélectionnez un flux vidéo compris entre 1 et 4 pour l'affichage de l'image en direct.

Instantané

Générez un enregistrement instantané (sans plug-in ActiveX)

Sortie digitale

Activez et désactivez manuellement la sortie digitale

Configuration

Configurez le serveur vidéo (réglages administrateur)

Réglages client

Configurez les réglages client. Vous trouverez plus de détails dans les pages suivantes.

Langue

Réglez la langue de l'interface.

Contrôle PTZ

Utilisez les boutons de contrôle PTZ digital et mécanique.

Ajustement de la taille de la fenêtre

Cette fonction permet d'ajuster l'image en direct grâce à 3 facteurs de zoom (100 %, 50 % et 25 %). Il est également possible d'ajuster l'image en direct automatiquement à la taille actuelle du navigateur. Pour ce faire, sélectionnez l'option « AUTO ».

Format de l'écran

Le bouton « 4:3 » permet de régler les proportions de l'image en direct sur 4:3.

Menu affiché/masqué

Cette fonction permet d'afficher ou de masquer le menu.

5.1 Commande audio/vidéo

Instantané

sauvegarder le fichier image sur votre ordinateur, effectuez un clic droit sur l'image et sélectionnez l'option « Enregistrer sous ».

Zoom digital et instantané

Cliquez sur l'icône Loupe sous l'affichage du serveur vidéo. Le pupitre de commande du zoom digital est alors affiché. Désactivez le champ de commande « Désactiver zoom digital » et modifiez le facteur de zoom avec le curseur.

Démarrage/arrêt de l'affichage de l'image en direct

Le flux en direct peut être interrompu ou arrêté. Dans les deux cas, le flux en direct peut être repris en cliquant sur l'icône Lecture.

Enregistrement local

Il est possible de lancer ou d'arrêter un enregistrement sur le disque dur local. Le chemin d'enregistrement est configuré dans « Réglages client ».

Ajustement du volume

Cliquez sur cette icône pour régler manuellement le niveau de la sortie audio.

Activation/désactivation de la fonction audio

Conversation

Tant que ce bouton est enfoncé, les signaux audio de l'ordinateur sont transférés à la sortie audio du serveur vidéo.

Volume du microphone

Cliquez sur cette icône pour régler manuellement le niveau de l'entrée audio du serveur vidéo.

Désactivation du son

Ce bouton permet d'activer ou de désactiver l'entrée audio du serveur vidéo.

Plein écran

Ce bouton permet d'activer la fonction plein écran. L'image en direct du serveur vidéo est affichée en plein écran.

5.2 Réglages client

Les réglages utilisateur sont sauvegardés sur l'ordinateur local. Les réglages suivants sont disponibles :

Les options média permettent à l'utilisateur de désactiver la fonction audio ou vidéo.

Les options de protocole permettent de sélectionner un protocole de connexion entre le client et le serveur. Plusieurs options de protocole sont disponibles pour optimiser l'application : UDP, TCP, HTTP.

Le protocole UDP permet d'obtenir un plus grand nombre de flux audio et vidéo en temps réel. Il est cependant possible que quelques paquets de données soient perdus en raison du grand nombre de données transitant sur le réseau. L'affichage des images manque donc de clarté. L'utilisation du protocole UDP est conseillée quand aucune exigence spécifique n'est requise.

Lors de l'utilisation du protocole TCP, le nombre de paquets de données perdus est plus faible et l'affichage vidéo est plus précis. L'inconvénient de ce protocole est cependant que le flux en temps réel est moins bon qu'avec le protocole UDP.

Sélectionnez le protocole HTTP si le réseau est protégé par un pare-feu et si seul le port HTTP (80) doit être ouvert.

La sélection du protocole est conseillé dans l'ordre suivant : UDP – TCP – HTTP

Les options de sauvegarde MP4 permettent à l'utilisateur d'ajuster le chemin du fichier pour la sauvegarde immédiate de données. Le bouton « Ajouter date et heure au nom de la donnée » génère des fichiers dont le nom se compose comme suit :

CLIP_20091115-164403.MP4
NomDeFichier-supplémentaire_AnnéeMoisJour-HeureMinuteSeconde.MP4

Options de sauvegarde MP4

Dossier: c:\Record Naviguer...

Préfixe du nom de donnée: CLIP

☑ Ajouter date et heure au nom de la donnée

Sauvegarder

Les données enregistrées peuvent être lues au moyen d'un lecteur vidéo capable de lire les fichiers MP4 (p. ex. VLC Mediaplayer).

6. Réglages administrateur

6.1 Système

Seul l'administrateur a accès à la configuration système. Toutes les catégories de la colonne de gauche sont décrites dans les pages suivantes. Les textes en gras correspondent aux données spécifiques sur les pages d'options. L'administrateur peut entrer l'URL indiquée sous l'illustration pour accéder directement à la page d'affichage de la configuration.

ABUS Security-Center

ABUS Security Tech Germany

Configuration

- Système
- Sécurité
- HTTPS
- SNMP
- Réseau
- DDNS
- Liste d'accès
- Audio et vidéo
- Détection de mouvement
- Détection de falsification de la caméra
- Commande caméra
- Application
- Enregistrement
- Sauvegarde locale
- Log de système
- Voir paramètres
- Maintenance

Version: 1210I

Home

Système

Nom hôte: TVIP40000 H.264 Video Server

☐ Eteindre l'indicateur LED

Heure système

Zone de temps: GMT+01:00 Amsterdam, Berlin, Rome, Stockholm, Viennes, Madrid, Paris

☐ Activer heure d'été:

Note: Vous pouvez charger vos règles de l'heure d'été sur la page Maintenance ou utiliser la valeur standard de la caméra.

◉ Maintenir date et heure actuelles

○ Synchroniser avec heure de l'ordinateur

○ Manuellement

○ Automatique

DI et DO

Entrée digitale: L'état actif est Faible , état actuel est **Haut**

Sortie digitale: L'état actif est Mise à la terre , état actuel est **Ouvert**

Sauvegarder

« Nom hôte » Le texte indique le titre sur la page d’accueil.

« Eteindre l’indicateur LED » Sélectionnez cette option pour éteindre l’indicateur LED du serveur vidéo. Ceci permet d’éviter que d’autres personnes remarquent que le serveur vidéo est en marche.

« Zone de temps » Adapte l’heure au fuseau horaire sélectionné.

« Activer heure d’été » Active les réglages de l’heure d’été dans le serveur vidéo. Tous les réglages de l’heure d’été de chaque fuseau horaire sont déjà sauvegardés dans le serveur vidéo.

« Maintenir date et heure actuelles » Sélectionnez cette option pour conserver la date actuelle et l’heure actuelle du serveur vidéo. Une horloge temps réel interne permet de conserver la date et l’heure du serveur vidéo même après une perte de tension.

« Synchroniser avec heure de l’ordinateur » Synchronise la date et l’heure du serveur vidéo avec l’ordinateur local. La date et l’heure protégées en écriture de l’ordinateur sont affichées après la mise à jour.

« Manuellement » La date et l'heure sont entrées par l’administrateur. Respectez le format de chaque champ lors de la saisie.

« Automatique » La date et l’heure sont synchronisées avec le serveur NTP par Internet à chaque démarrage du serveur vidéo. Ceci n’est pas possible lorsque le serveur d’horloge affecté n'est pas accessible.

« Serveur NTP » Affecte l’adresse IP ou la désignation de domaine du serveur d’horloge. Si le champ est laissé vide, le serveur vidéo est connecté aux serveurs d’horloge standard.

« DI et DO » Règle l’état prédéfini pour l’entrée d’alarmes et la sortie de relais.

N’oubliez pas de cliquer sur **« Sauvegarder »** pour que les modifications soient prises en compte.

6.2 Sécurité

« Mot de passe d.origine » Sert à modifier le mot de passe de l’administrateur par l’entrée d’un nouveau mot de passe. Pour des raisons de sécurité, la saisie de mots de passe est aveugle. Après avoir cliqué sur **« Sauvegarder** », le navigateur Internet invite l’administrateur à entrer le nouveau mot de passe pour accéder au serveur vidéo.

« Ajouter nouvel utilisateur » Entrez le nom du nouvel utilisateur et son mot de passe, puis cliquez sur **« Ajouter »**. Le nouvel utilisateur apparaît dans la liste des noms d’utilisateurs. Vous pouvez définir jusqu’à vingt comptes d’utilisateurs.

« Gérer utilisateur » Ouvrez la liste contenant les noms d’utilisateurs et recherchez l’utilisateur que vous souhaitez modifier, puis modifiez les données souhaitées. Cliquez sur **« Mise à jour »** pour que les modifications soient prises en compte.

« Supprimer utilisateur » Ouvrez la liste contenant les noms d’utilisateurs et recherchez l’utilisateur que vous souhaitez modifier, puis cliquez sur **« Supprimer »** pour supprimer l’utilisateur de la liste.

Gérer privilège

Administrateur : accès illimité au serveur vidéo.
Opérateur : pas d'accès à la fenêtre de configuration. Peut exécuter des commandes URL supplémentaires (p. ex. PTZ).
Utilisateur : l'accès est limité à la page d'accueil (visualisation en direct).

Sortie digitale : le groupe d'utilisateur peut commander les entrées et sorties d'alarmes.
Contrôle PTZ : le groupe d'utilisateurs a accès au contrôle PTZ.
Autoriser visualisation anonyme : ni nom d'utilisateur ni mot de passe n'est requis pour accéder à la page d'accueil.

6.3 HTTPS

Le protocole HTTPS est utilisé pour le chiffrement et l'authentification de la communication entre le serveur Web (serveur vidéo) et le navigateur (ordinateur client) sur le World Wide Web. Toutes les données qui sont transférées du serveur vidéo à l'ordinateur client sont chiffrées par SSL. Pour que le HTTPS fonctionne, il faut, outre le chiffrement SSL (compatible avec les navigateurs usuels), un certificat confirmant l'authenticité de la source.

Activer HTTPS
*Pour activer HTTPS, il faut créer et installer le certificat d'abord.
Activer connexion de sécurité HTTPS:
Sauvegarder
Créer et installer méthode de certificat
Créer certificat sous-signé automatiquement
Créer certificat sous-signé manuellement:
Créer demande de certificat et installer:
Information certificat
Etat: Pas installé
Caractéristiques Déplacer

« Activer connexion de sécurité HTTPS » Un accès non chiffré (HTTP) + chiffré (HTTPS) ou un accès exclusivement chiffré (HTTPS) peut être autorisé.

Quand une connexion sécurisée HTTPS est activée, il est possible d'accéder au serveur vidéo comme suit :
https:\\« adresse IP »
Pour obtenir une diffusion par connexion HTTPS, utilisez le lien suivant :
https:\\« adresse IP »:« port HTTPS »\Live.sdp

Créer et installer méthode de certificat

« Créer certificat sous-signé automatiquement » Un certificat prédéfini dans le serveur vidéo est utilisé. L'utilisateur ne peut effectuer aucun réglage.

« Créer certificat sous-signé manuellement » Un nouveau certificat est créé. Des données spécifiques doivent être entrées.

« Créer demande de certificat et installer » Cette option permet de créer une demande de certificat qui peut être transmise à une autorité de certification. Il est également possible d'installer un certificat provenant d'une autorité de certification reconnue (p. ex. VeriSign) sur le serveur vidéo.

Remarque : utilisez un « certificat sous-signé » lorsque vous recevez, par exemple, un avertissement de votre navigateur. Les certificats sous-signés sont toujours considérés comme non sécurisés par le navigateur Internet car ni certificat racine, ni preuve d'authenticité d'une autorité de certification ne sont disponibles.

6.4 SNMP

Le Simple Network Management Protocol est un protocole réseau permettant de surveiller et de commander des appareils en réseau (p. ex. routeur, serveur, commutateurs, imprimante, ordinateur) depuis un poste central. Ce protocole régule la communication entre les appareils surveillés et le poste de surveillance. Activez cette fonction lorsque vous utilisez un serveur de gestion SNMP dans votre réseau. Vous pouvez également vous servir de solutions logicielles qui peuvent être installées sur votre système informatique.

« Activer SNMPv1, SNMPv2c » En fonction des réglages de votre serveur SNMP, vous pouvez ici définir des champs de nom des groupes écrire/lire.

SNMP Configuration

☑ Activer SNMPv1, SNMPv2c

SNMPv1, SNMPv2c Réglages

Communauté avec lire/écrire : Private

Communauté seulement avec lecture: Public

☐ Activer SNMPv3

« Activer SNMPv3 » Si votre serveur SNMP supporte le protocole SNMP version 3, vous pouvez effectuer des interrogations d'état sécurisées. Un algorithme de chiffrement et un mot de passe doivent être sauve-gardés sur le serveur vidéo et sur le serveur SNMP pour pouvoir effectuer la requête des groupes écrire/lire.

6.5 Réseau

6.5.1 Réglages du réseau

Toutes les modifications effectuées dans cette page entraînent un redémarrage du système pour que ces modifications soient prises en compte. Assurez-vous que les champs sont correctement remplis avant de cliquer sur « Sauvegarder ».

« **LAN** » Le préréglage est LAN. Utilisez ce réglage quand le serveur vidéo est connecté par LAN. Des réglages supplémentaires comme l'adresse IP et le masque de sous-réseau sont nécessaires.

« Reprendre automatiquement l'adresse IP » A chaque redémarrage du serveur vidéo, cette adresse IP est assignée par un serveur DHCP.

« **Utiliser une adresse IP fixe** » Les données du réseau comme l'adresse IP sont des valeurs fixes.

« **Adresse IP** » Elle est nécessaire pour l'identification du réseau.

« **Masque de sous-réseau** » Il permet de déterminer si la destination se trouve dans le même sous-réseau. La valeur standard est « 255.255.255.0 ».

« **Routeur standard** » Il s'agit de la passerelle pour le transfert des images à un autre sous-réseau. Une configuration de routeur incorrecte empêche la transmission à ces destinations situées dans des sous-réseaux différents. En présence d'une connexion par câble CrossLink, entrez impérativement une adresse IP avec la même zone de sous-réseau que le serveur vidéo (p. ex. 192.168.0.1).

« **DNS primaire** » Serveur de la désignation de domaine primaire qui permet de transformer les noms d'hôtes en adresses IP.

« **DNS secondaires** » Serveur de la désignation de domaine secondaire pour la création d'une copie de sauvegarde du DNS primaire.

« **Utiliser l'UPnP** » Le service Universal Plug and Play est activé. Si votre système d'exploitation supporte le service UPnP, le serveur vidéo peut être directement sollicité par la gestion UPnP (Windows : Voisinage réseau).

Assurez-vous que l'option « Utiliser l'UPnP » est toujours activée. Le service UPnP est utilisé par Eytron VMS pour détecter le serveur vidéo.

« **Transfert de port UPnP activé** » Le transfert de port Universal Plug and Play pour les services réseau est activé. Si votre routeur supporte le service UPnP, cette option active automatiquement le transfert de port des flux vidéo côté routeur pour le serveur vidéo.

« PPPoE » Utilisez ce réglage quand le serveur vidéo est directement connecté à un modem DSL. Le nom d'utilisateur et le mot de passe vous sont fournis par votre fournisseur Internet (ISP).

« IPv6 » Utilisez cette fonction pour travailler avec des adresses IP de la génération v6.

☑ Activer IPv6

Information IPv6

☑ Lancer manuellement l'adresse IP

Adresse IP optionnelle / Longueur préfix [ ] / 64

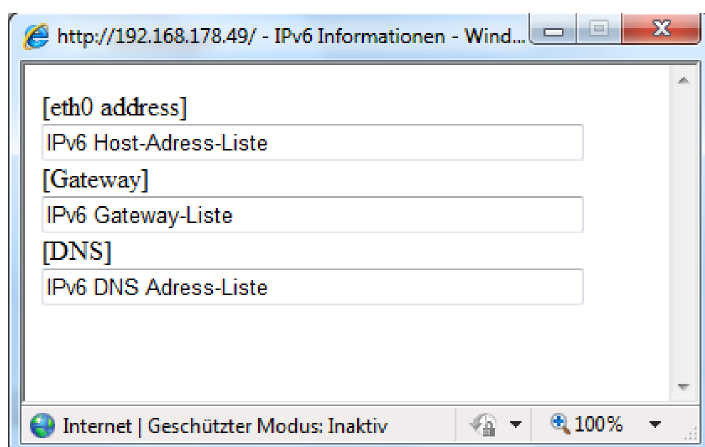
Routeur d'origine optionnel [ ]

DNS primaire optionnel [ ]

Assurez-vous que votre réseau et votre matériel supportent IPv6.

Quand IPv6 est activé, le serveur vidéo attend par défaut qu'une adresse IPv6 lui soit affectée par le routeur par le biais du DHCP.
En l'absence d'un serveur DHCP, définissez une adresse IP manuellement.
Pour ce faire, activez « Lancer manuellement l'adresse IP » et entrez l'adresse IP, le routeur par défaut et l'adresse DNS.

« Information IPv6 » Toutes les informations liées à l'IPv6 sont indiquées dans une fenêtre séparée..



Quand tous les réglages IPv6 sont corrects, vous pouvez les voir dans la fenêtre du bas.

[eth0 address]

2001:0c08:2500:0002:0202:d1ff:fe04:65f4/64@Global

fe80:0000:0000:0000:0202:d1ff:fe04:65f4/64@Link

[Gateway]

fe80::211:d8ff:fea2:1a2b

[DNS]

2010:05c0:978d::

6.5.2 IEEE 802.1x

Activez cette fonction quand votre voisinage réseau utilise la norme IEEE 802.1x (contrôle d'accès par port du réseau).
IEEE 802.1x améliore la sécurité des réseaux locaux.
Une connexion n'est autorisée que si tous les certificats entre le serveur et le « client » sont vérifiés. Ceci se fait au moyen d'un authentificateur sous forme de commutateur/point d'accès dont les requêtes sont envoyées au serveur d'authentification RADIUS.
Sinon, aucune connexion n'est établie et l'accès au port est refusé.

Assurez-vous que les composants de votre réseau et le serveur RADIUS supportent la norme IEEE 802.1x.

6.5.3 HTTP

« **Port HTTP** » Ce port peut varier du port par défaut 80 (80, ou 1025 - 65535). A l'issue de la modification du port, il convient d'informer l'utilisateur de la modification apportée afin de permettre l'établissement d'une connexion. Par exemple, si l'administrateur modifie le port HTTP du serveur vidéo dont l'adresse IP est 192.168.0.99 pour le faire passer de 80 à 8080, l'utilisateur doit entrer « http://192.168.0.99:8080 » au lieu de « http://192.168.0.99 » dans le navigateur Interne.

« **Port HTTP secondaire** » Port HTTP supplémentaire pour l'accès au serveur vidéo

Les noms d'accès suivants peuvent être réglés pour accéder directement à des flux vidéo sur Internet. L'accès se fait par des images comprimées JPEG et permet aux navigateurs Internet (Firefox, Netscape) qui ne peuvent pas traiter les plug-ins ActiveX d'avoir un accès direct au flux vidéo :

« Nom d'accès pour stream 1 » Nom d'accès pour le flux MJPEG 1.
« Nom d'accès pour stream 2 » Nom d'accès pour le flux MJPEG 2.
« Nom d'accès pour stream 3 » Nom d'accès pour le flux MJPEG 3.
« Nom d'accès pour stream 4 » Nom d'accès pour le flux MJPEG 4.

Remarque : Internet Explorer ne supporte pas la représentation d'images MJPEG sans Active X.

6.5.4 FTP

« **Port FTP** » Port du serveur FTP interne. Ce port peut varier du port par défaut 21 (21, ou 1025 – 65535). Les données vidéo sauvegardées sur le serveur vidéo peuvent être directement consultées via FTP. Utilisez un programme FTP autonome.

Le format de l'adresse pour l'entrée des données de connexion se construit comme suit :
Serveur : adresse IP du serveur vidéo
Nom d'utilisateur : utilisateur administrateur
Mot de passe : mot de passe de l'administrateur
Port : port FTP du serveur vidéo

Exemple (avec programme FTP)
Serveur : 192.168.0.99
Nom d'utilisateur : root
Mot de passe : admin
Port : 1026

Server: /mnt/auto/CF/NCMF

/
mnt
auto
CF
NCMF
ncmf
CF

Dateiname	Dateigröße	Dateityp	Zuletzt geändert	Berechtigu...	Besitzer/Gr...
000_1283513262.jpg	77.915	JPEG-Bild	03.09.2010 11:2...	-rwxr-xr-x	root root
000_1283513305.jpg	77.966	JPEG-Bild	03.09.2010 11:2...	-rwxr-xr-x	root root
000_1283513366.jpg	77.821	JPEG-Bild	03.09.2010 11:2...	-rwxr-xr-x	root root
000M.jpg	77.098	JPEG-Bild	03.09.2010 11:2...	-rwxr-xr-x	root root
001.jpg	77.218	JPEG-Bild	03.09.2010 11:2...	-rwxr-xr-x	root root
001M.jpg	77.259	JPEG-Bild	03.09.2010 11:2...	-rwxr-xr-x	root root
001M_1283513256.jpg	77.638	JPEG-Bild	03.09.2010 11:2...	-rwxr-xr-x	root root
001M_1283513303.jpg	78.269	JPEG-Bild	03.09.2010 11:2...	-rwxr-xr-x	root root
001M_1283513364.jpg	77.926	JPEG-Bild	03.09.2010 11:2...	-rwxr-xr-x	root root
002.jpg	77.267	JPEG-Bild	03.09.2010 11:2...	-rwxr-xr-x	root root
002_1283513268.jpg	78.236	JPEG-Bild	03.09.2010 11:2...	-rwxr-xr-x	root root
002_1283513310.jpg	78.411	JPEG-Bild	03.09.2010 11:2...	-rwxr-xr-x	root root
002_1283513368.jpg	77.496	JPEG-Bild	03.09.2010 11:2...	-rwxr-xr-x	root root
20100903_112614.mp4	542.681	MPEG-4 M...	03.09.2010 11:2...	-rwxr-xr-x	root root
20100903_112711.mp4	546.532	MPEG-4 M...	03.09.2010 11:2...	-rwxr-xr-x	root root
20100903_112819.mp4	547.002	MPEG-4 M...	03.09.2010 11:2...	-rwxr-xr-x	root root
normal-1283513308_2073467...	35.217.960	3GPP Movie	03.09.2010 11:2...	-rwxr-xr-x	root root
normal-1283513368_1099627...	2.565.197	3GPP Movie	03.09.2010 11:2...	-rwxr-xr-x	root root

19 Dateien und 2 Verzeichnisse. Gesamtgröße: 40.507.467 Bytes

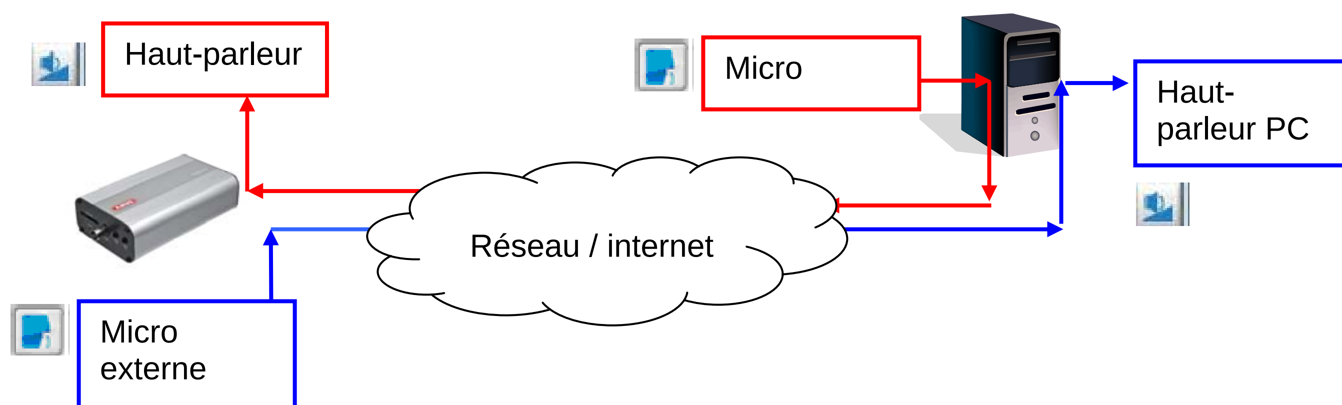
6.5.5 HTTPS

« **Port HTTPS** » Ce réglage de port sert pour le port HTTPS interne. Ce port peut varier du port par défaut 443 (443 ou 1025 – 65535). Vous trouverez des réglages HTTPS supplémentaires dans le chapitre 5.5.3.

6.5.6 Audio bidirectionnel

« Audio bidirectionnel » Ce port est utilisé pour la fonction audio bidirectionnel. Ce port peut varier du port par défaut 5060 (5060 ou 1025 – 65535).

Pour pouvoir utiliser la fonction audio bidirectionnel, vous devez activer MPEG-4/H.264 dans **« Vidéo et audio »** pour le flux vidéo sélectionné. Le format MJPEG supporte uniquement le transfert de données vidéo et n'est donc pas adapté pour cette fonction.



Fonction du flux en direct :

Lancez le transfert des données audio.
Règle la sensibilité de l'entrée audio du serveur vidéo.
Désactivez le micro/l'entrée audio.
Cliquez à nouveau sur le bouton pour arrêter la transmission audio.

6.5.7 Transfert RTSP

« **Authentification** » L'authentification peut être réglée sur en mode simple (Basic) ou avancé (Digest).

Si l'authentification RTSP est activée, le nom d'utilisateur et le mot de passe d'un utilisateur valide (p. ex. administrateur) doivent être entrés lors de la connexion RTSP.
REMARQUE : l'authentification RTSP doit être supportée par le lecteur vidéo (p. ex. Realplayer 10.

« **Nom d'accès pour stream 1** » Il s'agit du nom d'accès 1 permettant d'établir la connexion d'un client. Le type de codec doit être MPEG4 ! Utilisez
rtsp://<adresse IP>:port RTSP /<Nom d'accès 1> pour établir une connexion.

« **Nom d'accès pour stream 2** » Il s'agit du nom d'accès 2 permettant d'établir la connexion d'un client. Le type de codec doit être MPEG4 ! Utilisez
rtsp://<adresse IP>:port RTSP /<Nom d'accès 2> pour établir une connexion.

« **Nom d'accès pour stream 3** » Il s'agit du nom d'accès 3 permettant d'établir la connexion d'un client. Le type de codec doit être MPEG4 ! Utilisez
rtsp://<adresse IP>:port RTSP /<Nom d'accès 3> pour établir une connexion.

« **Nom d'accès pour stream 4** » Il s'agit du nom d'accès 4 permettant d'établir la connexion d'un client. Le type de codec doit être MPEG4 ! Utilisez
rtsp://<adresse IP>:port RTSP /<Nom d'accès 4> pour établir une connexion.

Accès RTSP avec VLC :
rtsp://192.168.0.99:10052/live.sdp

« **Port RTSP** » Ce port peut varier du port par défaut 554 (554 ou 1025 à 65535). En cas de modification, utilisez le même format que pour le port HTTP.

« **Port RTP pour vidéo** » Ce port peut varier du port par défaut 5558. Le numéro du port doit être un chiffre pair.

« **Port RTCP pour vidéo** » Ce port doit correspondre au « Port RTP pour vidéo » plus 1.

« **Port RTP pour audio** » Ce port peut varier du port par défaut 5556. Le numéro du port doit être un chiffre pair.

« **Port RTCP pour audio** » Ce port doit correspondre au « Port RTP pour audio » plus 1.

6.5.8 Multidiffusion

La multidiffusion est un transfert d'informations d'un point à un groupe (également nommée communication point à multipoint). L'avantage de la multidiffusion est qu'elle permet de transférer des informations simultanément à plusieurs participants ou à un groupe de participants donné sans que la bande passante ne soit multipliée par le nombre de destinataires lors de l'envoi. L'émetteur utilise la même bande passante pour la multidiffusion que pour l'envoi à un seul destinataire. Une multiplication des paquets se produit au niveau de chaque distributeur réseau (commutateur, routeur).

La multidiffusion permet d'envoyer des données performantes simultanément à de nombreux destinataires dans des réseaux IP. Des adresses multidiffusion spéciales sont utilisées. Dans IPv4, une zone d'adresse allant de 224.0.0.0 à 239.255.255.255 est réservée.

Les réglages multidiffusion suivants peuvent être configurés pour les flux 1 à 4 dans le serveur vidéo.

« **Toujours multicast** » Activez cette option pour utiliser la multidiffusion.

« **Adresse de groupe Multicast** » Définit un groupe d'hôtes IP appartenant à ce groupe.

« **Port vidéo Multicast** » Ce port peut varier du port par défaut 5560. Le numéro du port doit être un chiffre pair.

« **Port vidéo Multicast RTCP** » Ce port doit correspondre au « Port vidéo multidiffusion » plus 1.

« **Port audio Multicast** » Ce port peut varier du port par défaut 5562. Le numéro du port doit être un chiffre pair.

« **Port audio Multicast RTCP** » Ce port doit correspondre au « Port audio multidiffusion » plus 1.

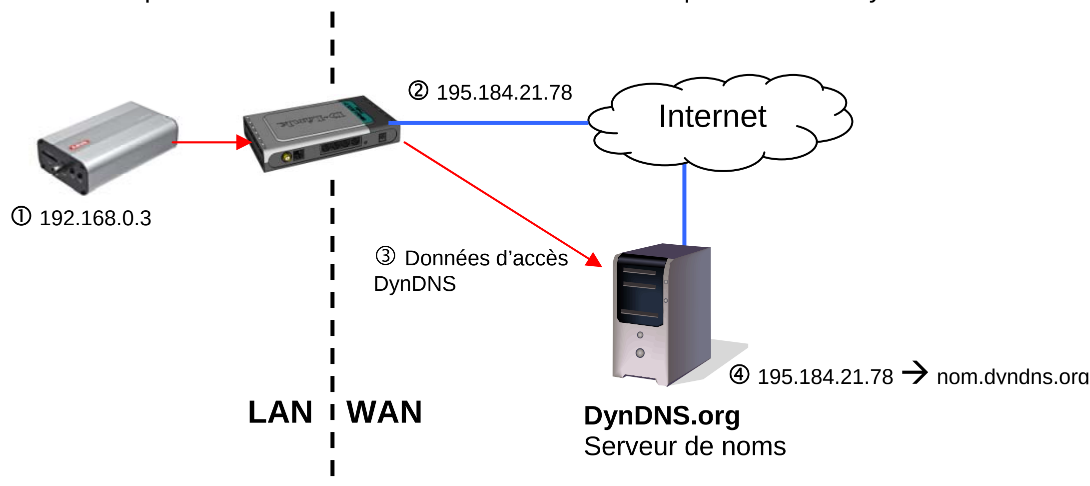
« **Multicast TTL** » Durée de vie du paquet.

Si vous définissez un transfert de port dans un routeur, tous les ports peuvent toujours être transférés (RTSP + HTTP). Ceci est nécessaire pour que la communication fonctionne.

7. DDNS

Le DynDNS ou DDNS (système de noms de domaine dynamique) est un système qui permet d'actualiser en temps réel les noms de domaines. Le serveur vidéo dispose d'un client DynDNS intégré qui peut exécuter de manière autonome l'actualisation de l'adresse IP auprès d'un fournisseur DynDNS. Si le serveur vidéo est raccordé à un routeur, nous vous conseillons d'utiliser la fonction DynDNS du routeur.

L'illustration représente l'accès/actualisation de l'adresse IP par le service DynDNS



« **Activer DDNS** » Cette option permet d'activer la fonction DDNS.

« **Fournisseurs d'accès Internet** » Cette liste de fournisseurs contient des hôtes fournissant des services DDNS. Etablissez une connexion avec la page du fournisseur de services pour être sûr que le service est disponible.

« **Nom hôte** » Ce champ doit être complété pour permettre l'utilisation du service DDNS. Entrez le nom d'hôte enregistré sur le serveur DDNS.

« **Nom d'utilisateur** » Le nom d'utilisateur et son adresse de messagerie doivent être indiqués dans ce champ pour permettre d'établir une connexion avec le serveur DDNS ou pour informer les utilisateurs de la nouvelle adresse IP. Remarque : si vous entrez le « nom d'utilisateur » dans ce champ, vous devez entrer le « mot de passe » dans le champ suivant.

« **Mot de passe** » Entrez votre mot de passe pour utiliser le service DDNS.

DDNS: Dynamic domain name service

Activer DDNS:

Fournisseur d'accès Internet: Dyndns.org(Dynamic)

Nom hôte:

Nom d'utilisateur:

Mot de passe:

Sauvegarder

7.1 Création d'un compte DDNS

Création d'un nouveau compte sur DynDNS.org

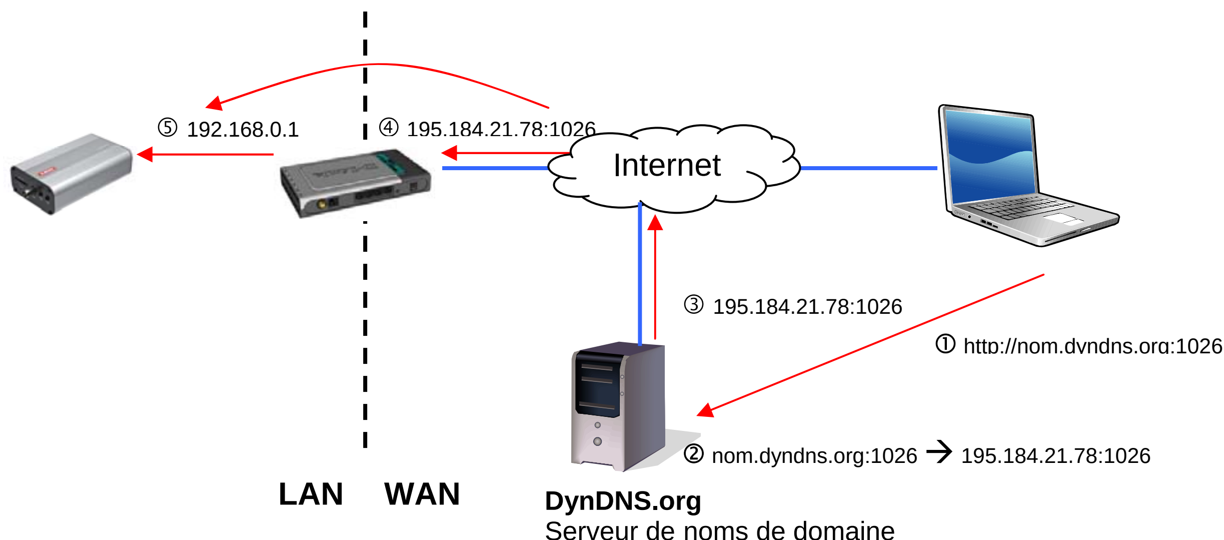
Saisie des informations du compte

Notez vos données utilisateur et saisissez-les dans la configuration du serveur vidéo.

7.2 Accès DDNS par routeur

Si le serveur vidéo en réseau est raccordé à un routeur, l'accès par DynDNS doit être configuré dans le routeur. Vous trouverez une description de la configuration DynDNS dans les routeurs pour les modèles courants de routeurs sur la page d'accueil d'ABUS Security-Center www.abus-sc.com.

L'illustration suivante représente l'accès à un serveur vidéo raccordé à un routeur par DynDNS.org.



Pour que l'accès DynDNS via un routeur fonctionne, un transfert de ports de tous les ports concernés (au moins RTSP + HTTP) doit être configuré dans le routeur.

8. Liste d'accès

Vous pouvez ici contrôler les accès au serveur vidéo au moyen de listes d'adresses IP.

« Nombre maximal de connexion(s) streaming est limité à » Nombre d'accès simultanés au serveur vidéo possible. En fonction de la bande passante disponible pour le serveur vidéo, il peut être utile de limiter l'accès.
« Activer filtre de liste d'accès » Active les filtres d'adresses IP définis dans « Filtre »

Vous pouvez définir le filtre d'adresses IP de deux manières différentes.

- Type de filtre « Autoriser » : seuls les adresses IP se trouvant dans la zone définie peuvent accéder au serveur vidéo.
- Type de filtre « nier » : les adresses IP se trouvant dans la zone définie ne peuvent pas accéder au serveur vidéo.

Cliquez sur « Ajouter » pour configurer les zones d'adresses. Les réglages suivants sont possibles :

Réglages généraux

Nombre maximal de connexion(s) streaming est limité à: 10 Voir information

Activer filtre de liste d'accès

Sauvegarder

Type Filtre

Autoriser nier

Sauvegarder

Filtre

Liste d'accès IPv4

Ajouter Supprimer

Administrateur adresse IP

Autoriser toujours l'adresse IP afin d'accéder au dispositif.

Sauvegarder

Règle : Unique, Valeur, Réseau :

- Unique : une adresse IP donnée est ajoutée.
- Valeur : une zone d'adresses IP « de – à » peut être définie.
- Réseau : des adresses IP avec des masques de sous-réseau donnés peuvent être définies.

Adresse filtre

Règle: Unique

Unique
Réseau
Valeur

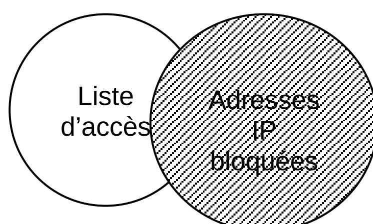
Adresse

OK Quitter

Exemple :
La zone d'adresses IP allant de 192.168.0.1 à 192.255.255.255 doit être autorisée.
Les adresses IP allant de 192.168.1.0 à 192.168.255.255 doivent être bloquées.

Résultat :
Seuls les accès de la zone d'adresses IP suivantes sont autorisés : 192.168.0.1 – 192.168.0.255.

Les accès autorisés et les adresses IP bloquées se recoupent toujours en partie.



9. Audio et vidéo

Home

Réglages vidéo

Titre vidéo:

Couleur: Couleur

Modulation: Automatique

Sélectionner stream cache: Stream 4

Orientation vidéo: Flip Miroir

Superposer titre et heure sur vidéo et instantané.

Réglages d'image | Masquage de zones privées

Réglages qualité vidéo pour stream 1:

Réglages qualité vidéo pour stream 2:

Réglages qualité vidéo pour stream 3:

Réglages qualité vidéo pour stream 4:

Réglages audio

Silencieux

Entrée de microphone externe: 0 dB

Type audio:

AAC:

Taux d'image AAC: 16 Kbps

GSM-AMR:

G.711:

Mode: pcmu

Sauvegarder

« **Titre vidéo** » Le texte apparaît dans la barre noire au-dessus de la fenêtre vidéo avec l'horodatage. L'horodatage (date et heure) est fournie par l'horloge temps réel intégrée du serveur vidéo.

« **Couleur** » Sélectionnez l'affichage en couleur ou l'affichage noir et blanc.

« Modulation » Sélectionnez soit le standard vidéo NTSC ou PAL, soit une reconnaissance automatique du signal vidéo par le serveur vidéo.

« Sélectionner stream cache » Le flux vidéo sélectionné est utilisé pour l'enregistrement de données vidéo avant et après alarme (voir section « Application »).

« **Flip »** Permet la rotation horizontale de la vidéo. Sélectionnez ces options si la caméra a été installée la tête en bas.

« **Miroir »** Permet la rotation verticale de la vidéo.

Utilisez les options Flip et Miroir quand la caméra est installée au plafond.

« Superposer titre et heure sur vidéo et instantané » Cette option permet d'afficher le titre et l'horodatage directement dans l'image vidéo et les instantanés. L'entrée du point « Titre vidéo » est utilisé.

9.1 Ajustement image

« Luminosité, Contraste, Saturation, Qualité »
Adaptez les valeurs à la luminosité.

Si vous modifiez la luminosité de la caméra, les réglages de l'image pour une mauvaise luminosité alors que la luminosité est bonne peuvent avoir une influence négative sur la qualité de l'image.

Pour visualiser les modifications du réglage de l'image, cliquez sur « Préface ». Pour appliquer les paramètres d'image définis, cliquez sur « Sauvegarder ». Cliquez sur « Restaurer » pour ignorer les modifications apportées.

9.2 Masquage de zones privées

Cette fonction permet de masquer des zones de l'image vidéo. Il est possible de sélectionner au maximum 5 zones, quelle que soit leur taille.

Dans un premier temps, activez cette zone en cochant la case **« Activer masquage de zones privées »**.

Cliquez sur le bouton **« Nouveau »** pour ouvrir une nouvelle fenêtre. Vous pouvez modifier la taille de cette fenêtre. Cliquez sur **« Sauvegarder »** pour conserver les réglages.

Cette fonction ne doit pas être activée quand la fonction PTZ / ePTZ de la caméra est utilisée. Cette fonction peut uniquement être configurée quand MS Internet Explorer est utilisé comme navigateur Internet (mode ActiveX).

9.3 Réglage de base

Options vidéo

Le serveur vidéo dispose de quatre flux vidéo à résolutions différentes pour permettre une utilisation plus flexible.

- Réglages qualité vidéo pour stream 1:
- Réglages qualité vidéo pour stream 2:
- Réglages qualité vidéo pour stream 3:
- Réglages qualité vidéo pour stream 4:

Réglages des flux 1, 2, 3 et 4
Vous pouvez configurer les flux 1 à 4 dans les menus correspondants.

La résolution du flux 4 est définie sur QCIF. Pour diffuser des images sur des appareils mobiles, utilisez le flux 4.

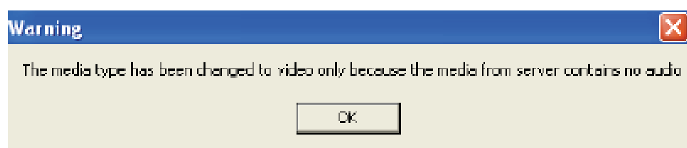
« Compression de l'image » Sélectionnez H.264, MPEG-4 ou MJPEG.
« Taille de l'image » Définissez ici la résolution souhaitée.
« Fréquence d'images max. » Définissez ici le débit des images.
« Intervalle trame clé » Détermine la fréquence de création d'i-frame. Plus l'intervalle est court, meilleure est la qualité de l'image, mais cela au prix d'une sollicitation plus élevée du réseau.
« Fréquence d'image fixe qualité vidéo » Définit une valeur fixe pour le débit des images. La qualité de l'image baisse lorsque la complexité de l'image augmente (p. ex. mouvement).
« Qualité d'image fixe » Définit une valeur fixe pour la qualité de l'image. La vitesse de transmission augmente lorsque la complexité de l'image augmente (p. ex. mouvement).

Compression → / Durée d'enregistrement ↓	**H.264**	**MPEG-4**	**MJPEG**
Séquence vidéo d'une minute en résolution D1 et qualité « bonne »	Env. **12** MB	Env. **14** MB	Env. **60** MB
Capacité de stockage **32 GB** carte SD	Env. **43** heures	Env. **36** heures	Env. **9** heures

Vous trouverez un tableau détaillé du réglage de la qualité en fonction de la résolution à la fin du manuel.

9.4 Réglages audio

« Silencieux » Toutes les fonctions audio du serveur vidéo sont désactivées. Un avertissement apparaît lors de l'accès au serveur vidéo.



« Entrée de microphone externe » Ajustez la valeur de +21 db à -33 db.

« Type audio » Sélectionnez ici le type audio et la vitesse de transmission souhaitée. Plus la valeur est élevée, plus la bande passante doit être importante :

- **« AAC** » (Advanced Audio Coding) Codec spécial pour la compression de données audio aux formats MPEG-4 et H.264.
- **« GSM-AMR »** (Global System for Mobile Communications – Adaptive Multi Rate) Codec vocal du réseau de téléphonie mobile GSM.
- **« G.711 »** Transmission en mode PCM (Puls Code Modulation) Mode pmca ou pmcu.

10. Détection de mouvement

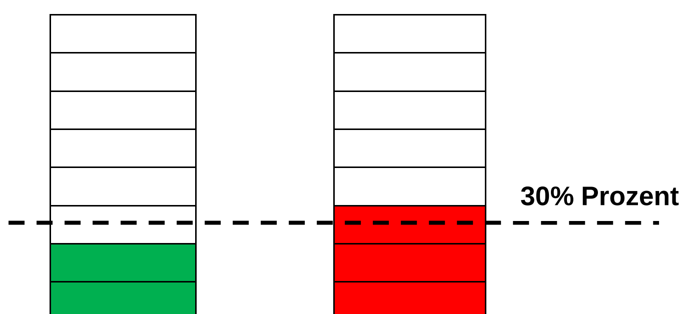
Il est possible d'activer jusqu'à trois zones de détection de mouvement dans le serveur vidéo. Sélectionnez **« Activer détection de mouvement »** pour effectuer la configuration.

La fonction de détection de mouvement n'est activée qu'une fois qu'une action est définie dans l'option de menu « Application ».

« Nom fenêtre » Le texte affiché dans ce champ apparaît en haut de la fenêtre.
« Sensibilité » Sensibilité en cas de modifications dans l'image (p. ex. sensibilité élevée : déclenchement par une modification faible de l'image).
« Pourcentage » Indique combien de pourcents de l'image doivent se modifier pour que le détecteur de mouvement se déclenche.

Cliquez sur le bouton **« Nouveau »** pour ajouter une nouvelle fenêtre. Pour redimensionner la fenêtre ou déplacer la barre de titre, effectuez un clic gauche sur la bordure de la fenêtre et maintenez le bouton de la souris enfoncé, puis déplacez la bordure de la fenêtre jusqu'à obtenir la taille souhaitée. Cliquez sur le 'x' dans le coin supérieur droit de la fenêtre pour fermer cette dernière.
Cliquez sur le bouton **« Sauvegarder »** pour sauvegarder les paramètres de la fenêtre correspondante.
Une barre graphique augmente ou diminue en fonction de la variation de l'image.

Une barre verte signifie que l'image varie au dessous du niveau de surveillance, tandis qu'une barre rouge signale une variation de l'image dépassant le niveau de surveillance. Si la barre est rouge, la fenêtre concernée apparaît également encadrée de rouge. La fenêtre surveillée disparaît au retour à la page d'accueil. Cependant, le cadre rouge est affiché dès qu'un mouvement est détecté.



Zone verte : un mouvement a été détecté mais n'entraîne pas le déclenchement d'une alarme.
Zone rouge : la variation de l'image (mouvement) est supérieure au seuil de 30 % et déclenche une alarme.

Fonctionnement de la détection de mouvement :

Deux paramètres permettent de régler la détection de mouvement : **Sensibilité** et **Pourcentage**. L'illustration explique comment ces deux paramètres influencent la détection de mouvement.

Un mouvement s'est produit entre l'image A et l'image B. Les modifications de pixels qui en résultent (en fonction du réglage de la sensibilité) sont représentées dans l'image C (en gris). Le réglage **« Sensibilité »** correspond à la capacité des détecteurs de reconnaître des mouvements dans l'image. Plus cette valeur est élevée, plus le nombre de modifications de pixels reconnues dans l'image est élevé. Lors d'une détection de mouvement, les modifications de pixels (en fonction de la sensibilité) sont sauvegardées sous forme de pixels d'alarme (champs roses dans l'image D) sur le serveur. Le seuil **« Pourcentage »** décrit le nombre de « pixels d'alarme » par rapport au nombre total de pixels dans la zone sélectionnée. Quand le nombre de pixels d'alarme défini (pourcentage) est atteint ou dépassé, une alarme est déclenchée. Pour que la détection de mouvement soit fiable, il est conseillé de définir une sensibilité élevée et un pourcentage faible.

11. Détection de falsification de la caméra

Le serveur vidéo supporte une fonction de détection de sabotage. Si la détection est activée, l'alarme en résultant peut être utilisée comme événement pour une notification (voir Application).

« Activer détection de caméra » Le détecteur est activé.

« Durée de déclenchement » La période définie depuis combien de temps un événement de sabotage doit exister avant que l'alarme ne se déclenche.

Les événements de sabotage suivants sont contrôlés :
- Torsion de la caméra
- Recouvrement de la caméra
- Modification de la mise au point de la caméra

Ces événements de sabotage peuvent être utilisés pour déclencher une notification dans la fonction de la caméra « Application/Réglage des événements ».

12. Commande de caméra

Le serveur vidéo offre la possibilité de commander une caméra PTZ analogique.

Réglages RS485

« Désactiver » La commande RS485 est désactivée.

« Caméra PTZ » Entrez ici les paramètres correspondants pour la caméra PTZ. Les protocoles suivants sont supportés : Pelco-D, Pelco-P, Samsung scc643, DynaDome/SmartDOME, Lilin PIH-7x00.
Si la caméra PTZ ne supporte aucun de ces protocoles, sélectionnez « Custom camera ».

« Tunnel HTTP transparent » Supporte les commandes RS485 de votre appareil PTZ via une interface réseau. Vous devez utiliser les paramètres nécessaires indiqués dans le manuel d'utilisation de votre appareil PTZ.

Réglages RS485

Désactiver
Caméra PTZ
Tunnel HTTP transparent

ID caméra: 1
Driveur PTZ: Pelco D protocol
Réglages port:
Baud: 2400
Bits de données: 8
Bits d'arrrêt: 1
Bit de parité: Aucun

Position preset | Commande adaptée

Sauvegarder

Utilisez les commandes PTZ indiquées dans le manuel d'utilisation de votre appareil PTZ.

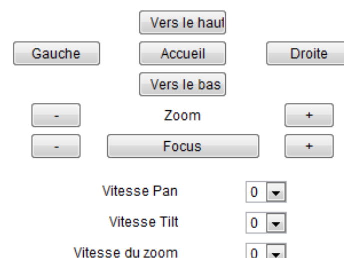
« ID caméra » Définit l'ID de la caméra.
« Driveur PTZ » Définit le protocole de l'appareil PTZ raccordé.
« Baud » Réglez la vitesse en bauds appropriée.
« Bits de données » Réglez les bits de données appropriés.
« Bits d'arrêt » Réglez les bits d'arrêt appropriés.
« Bit de parité » Définit la parité.

Sélection commande

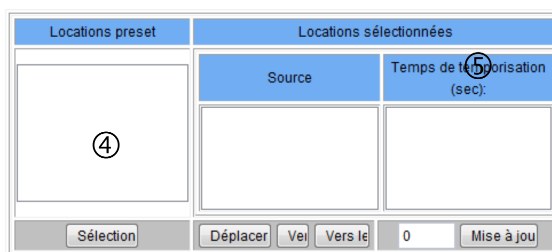
Vous pouvez sauvegarder 20 positions prédéfinies dans le serveur vidéo. Procédez comme suit :

1. Positionnez l'image de la caméra aux réglages souhaités au moyen des touches de direction.
2. Donnez un nom prédéfini à la position actuelle et cliquez sur Ajouter. Le nom apparaît dans liste de positions prédéfinies.
3. Répétez les étapes 1 et 2 pour définir d'autres positions prédéfinies.
4. Sélectionnez les positions prédéfinies pour lesquelles vous souhaitez utiliser une commande et confirmez avec « Sélectionner ».
5. Adaptez le temps d'arrêt de chaque position prédéfinie si nécessaire.
6. Sauvegardez les réglages.

①



②



Pour lancer la commande, appuyez sur « PATROL » dans l'image en direct du serveur vidéo. Pour l'arrêter, appuyez sur « STOP ».

Commande adaptée

L'option de menu « Commande adaptée » vous permet d'accéder directement à des fonctions données de votre appareil PTZ ou de votre caméra PTZ.
En général, cette fonction est utilisée pour ouvrir des positions prédéfinies ou des commandes prédéfinies.

Commande adaptée

Un champ "Nom de touche" vide signifie que la touche de commande ne sera pas affichée sur la page d'accueil.

	Nom de touche	Commande
Commande 1:	Tour 1	FF01000900010B
Commande 2:		
Commande 3:		
Commande 4:		
Commande 5:		

Sauvegarder | Fermer

A l’aide de cette fonction, vous pouvez créer des touches de commande dans l’image en direct du serveur vidéo pour l’utilisation/le réglage de l’appareil PTZ raccordé.
La fonction de chaque touche est décrite par un code hexadécimal (selon le protocole PTZ).
Toutes les caméras dôme GV d’ABUS utilisent le protocole PELCO D/P.
Vous pouvez créer jusqu’à 5 touches personnalisées.
Entrez le nom de la touche dans « Nom de touche » (p. ex. Tour 1).

Si vous avez entré le protocole de caméra « Caméra personnalisée », vous devez définir les fonctions de base comme « Vers le haut », « Vers le bas », « Gauche », « Droite » dans « Commande adaptée ». Vous trouverez les codes correspondants dans le manuel de l’appareil PTZ.

Si vous n’entrez pas de nom de touche, la touche n’apparaît pas dans l’image en direct.

Le protocole Pelco D/P fonctionne uniquement avec des chiffres hexadécimaux.

Entrez le code hexadécimal de la fonction souhaitée dans « Commande ».
(p. ex. FF 01 00 09 00 01 0B**)**

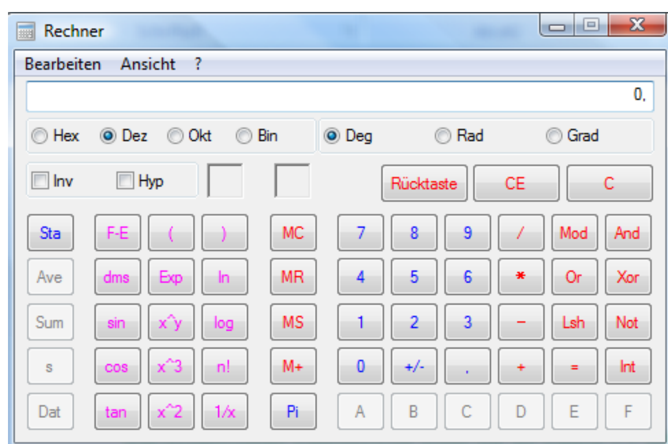
Le code ne doit pas contenir d'espaces ou de caractères spéciaux.
FF 01 00 09 00 01 0B → FF01000900010B

Explication des chiffres hexadécimaux
Le chapitre suivant décrit le système hexadécimal à l'aide de quelques exemples.

Decimal	Hex	Decimal	Hex	Decimal	Hex
1	1	11	B	30	1E
2	2	12	C	40	28
3	3	13	D	50	32
4	4	14	E	60	3C
5	5	15	F	70	46
6	6	16	10	80	50
7	7	17	11	90	5A
8	8	18	12	100	64
9	9	19	13	500	1F4
10	A	20	14	1000	3E8

Le système hexadécimal se base sur les chiffres de 0 à 9 et les lettres de A à F. Lors du calcul des sommes de contrôle, il faut prendre en compte que le chiffre hexadécimal est additionné.

La calculatrice de Microsoft Windows (en mode « scientifique ») est utile pour convertir des chiffres décimaux en chiffres hexadécimaux et pour additionner des chiffres hexadécimaux.



Commandes dôme pour TV7600, TV6702, TV7604 (Pelco)

Composition des commandes

Mot 1	Mot 2	Mot 3	Mot 4	Mot 5	Mot 6	Mot 7
Bit de synch. (toujours FF)	Adresse (ID de la caméra analogique)	Commande 1	Commande 2	Donnée 1	Donnée 2	Somme de contrôle Mots 2 à 6

Calcul des sommes de contrôle :

Mot 7 = Mot 2 + Mot 3 + Mot 4 + Mot 5 + Mot 6

Explication des mots :

« Mot 1 » toujours définit par « FF ».
« Mot 2 » définit l'ID de la caméra analogique.
« Mot 3 » et « Mot 4 » définissent les différentes fonctions PTZ (« position prédéfinie », « lancer commande », etc.)
« Mot 5 » et « Mot 6 » définissent par exemple la numérotation des positions prédéfinies et des commandes. Lorsque vous souhaitez utiliser une position prédéfinie, il faut également définir quel numéro de préréglage doit être utilisé.
« Mot 7 » est la somme de mot 2 à mot 6, également nommé somme de contrôle.

Exemple : « Aller à Preset 1 » correspond à la commande : FF 01 00 07 00 **01** 09

Mot 1 est toujours définit par FF.
Mot 2 est toujours l'ID du dôme GV.
Mot 3 et Mot 4 définissent la fonction : « Aller à Preset »
Mot 5 et Mot 6 définissent quelles positions prédéfinies doivent être utilisées.
Mot 7 est la somme de contrôle.

Explication : dans le mot 6, le chiffre hexadécimal 01 correspond à la position prédéfinie 1.
Pour utiliser la position prédéfinie 15, il faut que le mot 6 corresponde à 0F.

Exemple : « Aller à Preset 15 » correspond à la commande : FF 01 00 07 00 **0F** 17
La façon de procéder est similaire pour la sélection des commandes ou d'autres structures de fonctions dénombrables.

N'oubliez pas de recalculer la somme de contrôle après chaque modification de la commande.
Une modification de la commande dans l'exemple ci-dessus de Preset 1 à Preset 15 aurait pour conséquence d'augmenter la somme de contrôle de 14 !

Aperçu des commandes :

Commande	Mot 3	Mot 4	Mot 5	Mot 6
A partir de	00	10	00	2A
Vers le haut	00	08	00	3C
Gauche	00	04	2E	00
Droite	00	02	06	00
Arrêter	00	00	00	00
Menu	00	11	00	00
Commande	00	00	09	01 à 08
Balayage	00	0F	00	01
Zoom in	00	20	00	01
Zoom out	00	40	00	01
Focus près	01	00	00	01
Focus loin	00	80	00	00
Diaphragme fermé	04	00	00	00
Diaphragme ouvert	02	00	00	00
Sauvegarder Preset	00	03	00	01 à C8
Supprimer Preset	00	05	00	01 à C8
Aller à Preset	00	07	00	01 à C8
Régler aux.	00	09	00	01 à 08
Supprimer aux.	00	0B	00	01 à 08
Reset distant	00	0F	00	00
Début réglage zone	00	11	00	01 à 08
Fin réglage zone	00	13	00	01 à 08
Car. blancs sur écran	00	15	Position X 00 à 28	Valeur ASCII
Effacer écran	00	17	00	00
Acquitter alarme	00	19	00	N° alarme
Scan zone ON	00	1B	00	00
Scan zone OFF	00	1D	00	00
Config. démarrage modèle	00	1F	00	00
Config. arrêt modèle	00	21	00	00
Enlever modèle	00	23	00	00
Régler vitesse zoom ON	00	25	00	00 à 03
Régler vitesse focus ON	00	27	00	00 à 03
Réglage usine caméra	00	29	00	00
Autofocus auto/ON/OFF	00	2B	00	00-02
Diaphragme auto auto/ON/OFF	00	2D	00	00-02
AGC auto/ON/OFF	00	2F	00	00-02
BLC ON/OFF	00	31	00	01-02
Equ. blancs auto ON/OFF	00	33	00	01-02

13. Application

Vous pouvez ici automatiser des tâches dans le serveur vidéo. La configuration de l’application se compose de 3 zones : Evénement, Serveur, Médium. Un exemple type d’application peut se définir comme suit : en raison d’une détection de mouvement (événement), un e-mail (serveur) est envoyé à un utilisateur avec une image d’alarme (médium).

Réglages événement

Cliquez sur **« Ajouter »** pour créer un nouvel événement. Vous pouvez définir jusqu'à 3 événements.

« Nom événement » Entrez un nom unique sous lequel vous sauvegardez la configuration de l'événement.
« Activer cet événement » Cochez cette option pour activer l'événement programmé.
« Priorité » Les événements dont la priorité est plus élevée sont traités en premier.
« Détecter événement suivant après xx seconde(s) » Temps de pause entre des événements (p. ex. en cas de détection de mouvement).

Nom événement:

Activer cet événement

Priorité: Normal

Détecter événement suivant après 10 seconde(s).

Note: Ceci peut seulement être assigné à la détection de mouvement et l'entrée digitale

Déclencher

- Détection de mouvement vidéo
- Périodiquement
- Entrée digitale
- Redémarrage système
- Notification enregistrement
- Détection de falsification de la caméra
- Perte vidéo
- IP changé
- Video restore

Horaire événement

Dim Lun Mar Mer Jeu Ven Sam

Heure

- Toujours
- De 00:00 à 24:00 [hh:mm]

Action

Déclencher sortie numérique pour 1 secondes

Backup media if the network is disconnected

Déplacer à la destination preset:

Note: Veuillez configurer Locations preset premier

Ajouter serveur | Ajouter médium

	Serveur	Médium	Paramètre supplémentaire
	SD	-----None-----	Test SD Vue
	NAS	-----None-----	Créer les dossiers automatiquement Dossier personnalisé %IP/%Y%M%D/%H_MeinBeispieltext Vue

Sauvegarder | Fermer

13.1 Réglages déclenchement

« Détection de mouvement vidéo » Activez la fenêtre de mouvement souhaitée.
« Périodiquement » L'événement est déclenché périodiquement. Le réglage maximal est 999 minutes.
« Entrée digitale » Définit un signal qui se déclenche lors de l'entrée d'une alarme (p. ex. contact avec une porte).
« Redémarrage système » L'événement est déclenché lors du redémarrage du serveur vidéo (après une perte de tension).
« Notification enregistrement » Si la mémoire cible (médium) est pleine ou si une mémoire circulaire est écrasée, une alarme se déclenche.
« Détection de falsification de la caméra » Une alarme est déclenchée quand un sabotage de la caméra analogique raccordée est détecté.
« **Perte vidéo »** Une alarme est déclenchée quand le signal vidéo est interrompu.
« IP changé » Dès qu'une nouvelle adresse IP est affectée au serveur vidéo, une alarme est déclenchée.
« Video restore » Emet une alarme après une interruption suivie d'une réstauration du signal vidéo.

Horaire événement

« **Dim** » – « **Sam** » Permet de définir quels jours de la semaine un événement est exécuté.
« **Toujours** » Active l'événement quelle que soit l'heure (24 heures).
« **De** » – « **à** » L'événement est limité dans le temps.

13.2 Configuration du serveur

Vous pouvez sauvegarder jusqu'à 5 serveurs dans la caméra réseau. Cliquez sur **« Ajouter »** pour configurer un nouveau serveur. Le serveur de type **« SD »** est prédéfini et désigne la carte SD comme destination pour la sauvegarde des données. Les types de serveurs suivants peuvent être configurés :

- E-mail : entrez les données d'accès ici.
- FTP : entrez les données d'accès ici. Convention de l'adresse : ftp.abus-sc.com
- HTTP : entrez les données d'accès ici. Convention de l'adresse : http://abus-sc.com/cgi-bin/upload.cgi
- Dossier réseau : convention de l'adresse : \\192.160.0.5\NAS

Nom serveur:

Type serveur

E-mail:

Adresse e-mail émetteur:

Adresse e-mail destinataire:

Adresse serveur:

Nom d'utilisateur:

Mot de passe:

Port serveur 25

Ce serveur nécessite une connexion sécure (SSL).

FTP:

HTTP:

Sauvegarde de réseau:

Test | Sauvegarder | Fermer

Après avoir entré les données d'accès, sauvegardez les réglages. Avant de fermer la fenêtre, il est conseillé d'exécuter un **« Test »**. Le résultat est affiché dans une nouvelle fenêtre du navigateur.

13.3 Réglages médium

Vous pouvez sauvegarder jusqu'à 5 réglages de média dans le serveur vidéo.

Nom médium: ABUS

Type médium

- (●) Instantané
  - Source: Stream1
  - Envoyer 1 Image(s) avant événement [0~7]
  - Envoyer 1 Image(s) après événement [0~7]
  - Préfixe du nom de donnée:
  - [ ] Ajouter date et heure au nom de la donnée
- ( ) Clip vidéo
- ( ) Log de système
- ( ) Custom Message

[Sauvegarder] [Fermer]

« **Nom médium** » Nom unique du médium.

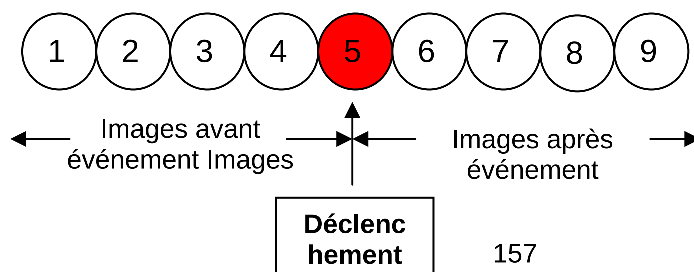
Il existe 4 différents types de média :

- Instantané (format de fichier JPEG)
- Clip vidéo (format de fichier MP4)
- Log de système (format de fichier TXT)
- Custom Message (format de fichier TXT)

Chaque médium défini ne doit être relié qu'à un seul événement.
Si un médium est relié à plusieurs événements, le fonctionnement du serveur vidéo sera perturbé.
Si vous souhaitez utiliser le même type de médium pour deux événements différents, vous devez dans un premier temps définir deux types de média séparés.

Instantané

« **Source** » Les flux vidéo 1 à 4 peuvent être enregistrés.
« **Envoyer image(s) avant événement** » Nombre d'instantanés avant un événement.
« **Envoyer image(s) après événement** » Nombre d'instantanés après un événement.



« **Préfixe du nom de donnée** » Entrez ici une désignation qui se trouvera devant le nom du fichier de l'instantané.
« **Ajouter date et heure au nom de la donnée** » Cette option permet d'ajouter la date et de l'heure au nom de l'instantané capturé afin de permettre de distinguer facilement le mode séquentiel du mode de déclenchement par événement. Par exemple « video@20030102_030405.jpg » signifie que l'image JPEG a été capturée le 2 janvier 2003 à 3 heures 4 minutes et 5 secondes. En l'absence de ce suffixe, le fichier nommé « video.jpg » est mis à jour sur le serveur FTP externe à expiration de l'intervalle indiqué.

Le nom du fichier est construit comme suit :
Préfixe_AAAAMMJJ_HHMMSS : ABUS_20091115_164501

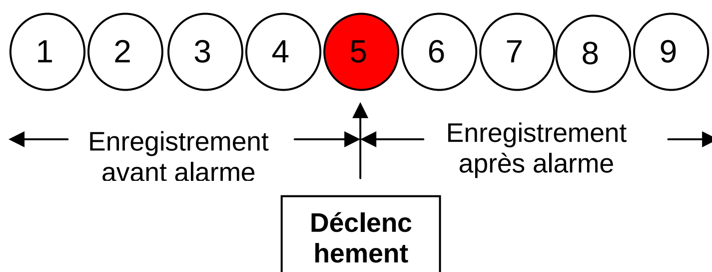
- Préfixe : voir Préfixe du nom de donnée.
- A : caractère générique pour année, AAAA = 2009
- M : caractère générique pour mois, MM = 11
- J : caractère générique pour jour, JJ = 15
- H : caractère générique pour heure, HH = 16
- M : caractère générique pour minute, MM = 45
- S : caractère générique pour seconde, SS = 01

Clip vidéo

« **Source** » Les flux vidéo 1 à 4 peuvent être enregistrés.

Le flux vidéo sélectionné pour l'option « Sélectionner stream cache » dans « Audio et vidéo » est proposé comme source.

« Enregistrement avant alarme » Intervalle des enregistrements avant alarme en secondes (max. 9 secondes).
« Durée max. » Durée maximale par fichier (max. 10 secondes).



« Taille de fichier max. »Taille maximale du fichier en ko (max. 800 ko).
« **Préfixe du nom de donnée** » Entrez ici une désignation qui se trouvera devant le nom du fichier de l'enregistrement vidéo (pour plus de détails, voir Instantané).

Log de système
Sauvegarde le contenu du log de système actuel dans un fichier texte.

Custom Message
Un message personnalisé est envoyé sous forme de fichier texte.

13.4 Action

Action

Déclencher sortie numérique pour 1 secondes

Backup media if the network is disconnected

Déplacer à la destination preset

Note: Veuillez configurer Locations preset premier

Ajouter serveur | Ajouter médium

	Serveur	Médium	Paramètre supplémentaire
	SD	-----None-----	Test SD · Vue
	NAS	-----None-----	Créer les dossiers automatiquement Dossier personnalisé %IP/%Y%M%D/%H_MeinBeispieltext Vue

Sauvegarder | Fermer

Configurez ici l'action qui doit être exécutée en présence d'une alarme déclenchée.
« Déclencher sortie numérique pour » Lors de l'activation, la sortie relais du serveur vidéo est activée.
« Déplacer à la destination preset » Une position prédéfinie est utilisée en cas d'alarme.
« **Serveur** » Le médium sélectionné est envoyé à un serveur donné (p. ex. un e-mail est envoyé avec un instantané).

« Créer les dossiers automatiquement » Créé automatiquement les dossiers dans le répertoire du lecteur réseau.
« Dossier personnalisé » Une désignation spécifique du dossier est définie au moyen de variables. Utilisez les variables disponibles dans le tableau ci-dessous.

Symbole	Exemple/fonction
/	*Créer un nouveau sous-dossier*
%IP = adresse IP	*192.168.0.1*
%N = nom événement	*Motion_W1*
%Y = année	*2010*
%M = mois	*03*
%D = jour	*04*
%H = heure	*14*
« _MeinBeispieltext »	*« _MeinBeispieltext »*

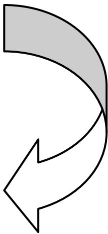
Exemple :
L'entrée suivante crée ce chemin.

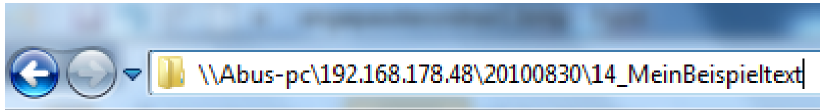
Créer les dossiers automatiquement

Dossier personnalisé

%IP/%Y%M%D/%H_MeinBeispieltext

Vue





13.5 Aperçu de l'applicatio

Vous trouverez dans cette section comment effecuter les réglages du serveur vidéo pour « Evénement », « Type médium » et « Type serveur ».
Vous pouvez y contrôler les différents réglages, les supprimer et en ajouter de nouveaux.
En outre, vous pouvez contrôler les différents paramètres comme Nom, Etat, Déclencher, Localité, Adresse.

Réglages événement

Nom	Etat	Dim	Lun	Mar	Mer	Jeu	Ven	Sam	Heure	Déclencher
ABUS	ON	V	V	V	V	V	V	V	00:00~24:00	boot

Ajouter ABUS Supprimer Aide

Réglages serveur

Nom	Type	Adresse/Localité
NAS	ns	\\my_nas\disk\folder

Ajouter Supprimer

Réglages médium

Capacité de mémoire disponible: 9550KB

Nom	Type
Snapshot	snapshot

Ajouter Supprimer

14. Enregistrement

La zone Enregistrement sert à créer des enregistrements à la différence qu'il est ici possible de définir des enregistrements vidéo permanents pour carte SD ou partages réseau. Vous pouvez sauvegarder deux réglages enregistrement dans le serveur vidéo. Pour créer un nouvel enregistrement, cliquez sur **« Ajouter ».**

Nom enregistrement: Video

Activer cet enregistrement

Priorité: Normal

Source: Stream1

Déclencher

Horaire

Network fail

Horaire enregistrement

Dim Lun Mar Mer Jeu Ven Sam

Heure

Toujours

De 00:00 à 24:00 [hh:mm]

Destination SD

Remarque: Pour activer la notification d'enregistrement, veuillez configurer. Application premier

Destination : **« Lecteur réseau »**

Destination NAS

Capacité:

Espace disponible totale

Espace réservée: 15 Mbytes

Préfixe du nom de donnée:

Créer les dossiers automatiquement

Dossier personnalisé : %Y%M%D/%H

Activer enregistrement cyclique

Remarque: Pour activer la notification d'enregistrement, veuillez configurer. Application premier

Sauvegarder Fermer

« **Nom enregistrement** » Nom unique d'un enregistrement.
« **Activer cet enregistrement** » Cocher cette case pour activer l'enregistrement.
« **Priorité** » Les enregistrements dont la priorité est plus élevée sont traités en priorité.
« **Source** » Les flux vidéo 1 à 4 peuvent être enregistrés.
« Horaire » L'horaire de l'enregistrement est utilisé.
« Network fail » En cas d'erreur réseau, la sauvegarde des données sur la carte SD est activée automatiquement.
« **Dim** » – « **Sam** » Permet de définir quels jours de la semaine un enregistrement est exécuté.
« **Toujours** » Active l'enregistrement quelle que soit l'heure.
« **De** » – « **à** » L'enregistrement est limité dans le temps.
« **Destination** » Carte SD ou dossier réseau.
« **Capacité**" L'espace de stockage maximal disponible sur la mémoire cible est utilisé.
« **Espace réservé** » Indique combien d'espace de stockage libre en MB est réservé.

Pour plus d'informations sur « Créer les dossiers automatiquement », référez-vous au chapitre 13.4 Action.
Si la fonction « Dossier personnalisé » est activée, la fonction « Activer enregistrement cyclique » ne peut pas être utilisée.

« Activer enregistrement cyclique » Active la fonction de mémoire circulaire. Si la valeur définie est atteinte lors de la sauvegarde des données, les données les plus anciennes sont écrasées.

Aperçu de l'enregistrement

« Nom (vidéo) » Ouvre la fenêtre de configuration de l'enregistrement.
« Etat (ON) » Règle l'état de l'enregistrement sur ON/OFF.
« **Destination (SD) »** Ouvre une liste détaillée contenant les enregistrements sauvegardés.

Réglages enregistrement

Nom	Etat	Dim	Lun	Mar	Mer	Jeu	Ven	Sam	Heure	Source	Destination
ABUS	ON	V	V	V	V	V	V	V	00:00~24:00	stream1	SD

Ajouter Test SD ABUS Supprimer

15. Mémoire locale

Cette section explique comment gérer la mémoire locale (carte SD) du serveur vidéo. Les cartes de type SD/SDHC classe 6 d'une capacité allant jusqu'à 32 GB peuvent être utilisées.

Gestion carte SD

Gestion carte SD

Etat carte SD: Prêt

Grandeur totale:	3860600 KBytes	Espace libre:	3647280 KBytes
Grandeur utilisée:	213320 KBytes	Utiliser (%):	5.526 %

Format

Contrôle carte SD:

- [ ] Activer sauvegarde cyclique
- [ ] Activer effacement automatique du disque

Durée maximale pour maintenir des données: 7 jours

Sauvegarder

Utilisez la fonction « **Format** » lorsque vous utilisez la carte pour la première dans le serveur vidéo.

Activez l'option « **Activer sauvegarde cyclique** » si les données les plus anciennes doivent être écrasées en premier quand la capacité de stockage de la carte SD est atteinte.

Activez l'option « **Activer effacement automatique du disque** » pour que la carte SD soit entièrement effacée après l'entrée de la durée de disponibilité maximum.

Chercher et voir les enregistrements

Si aucun critère n'est sélectionné, tous les enregistrements sont affichés dans la liste des résultats.

Chercher et voir les enregistrements

Attributs donnée:

Type déclenchement:	☐ Entrée numérique	☐ Perte vidéo	☐ Video restore
	☐ Redémarrage système	☐ Notification enregistrement	☐ Mouvement
	☐ Périodiquement	☐ Réseau échoué	☐ IP changé
	☐ Manipulation		
Type médium:	☐ Clip vidéo	☐ Instantané	☐ Texte
Bloqué:	☐ Bloqué	☐ Débloqué	

Heure de déclenchement:

De:	Date		Heure	
à:	Date		Heure	
		(yyyy-mm-dd)		(hh:mm:ss)

Chercher

« Type déclenchement » Sélectionnez un ou plusieurs critères selon lesquels un enregistrement se produit sur la carte SD.
« Heure de déclenchement » Sélectionnez la période souhaitée.

Cliquez sur « Chercher ». Tous les enregistrements correspondant aux critères sélectionnés sont affichés dans la liste des résultats.

Liste des résultats

Nombre d'éléments sur une page

Chercher résultats

Show 10 entries — Search: — Recher

	Heure de déclenchement	Type médium	Type déclenchement	Bloqué
☐	2010-01-02 10:44:13	Clip vidéo	Périodiquement	Non
☐	2010-01-02 10:45:13	Clip vidéo	Périodiquement	Non
☐	2010-01-02 10:46:13	Clip vidéo	Périodiquement	Non
☐	2010-01-02 10:47:13	Clip vidéo	Périodiquement	Non
☐	2010-01-02 10:48:13	Clip vidéo	Périodiquement	Non
☐	2010-01-02 10:49:12	Clip vidéo	Périodiquement	Non
☐	2010-01-02 10:50:12	Clip vidéo	Périodiquement	Non
☐	2010-01-02 10:51:11	Clip vidéo	Périodiquement	Non

Showing 1 to 8 of 8 entries — Défilement des pages

Vue | Télécharger | Déverouiller tout | JPEGs vers AVI | Bloquer/débloquer | Déplacer

« Vue » Affiche l'enregistrement sélectionné dans une nouvelle fenêtre.
« Télécharger » Invite à télécharger l'enregistrement sélectionné.
« JPEGs vers AVI » Plusieurs enregistrements d'images JPEG peuvent être sélectionnés (case à cocher) et sont convert's en fichier AVI.
« Bloquer/débloquer » Les enregistrements sélectionnés sont bloqués. Les enregistrements bloqués ne sont pas écrasés lors de la sauvegarde cyclique. Le déblocage supprime cet attribut.
« Déplacer » L'enregistrement sélectionné est supprimé.

Vous pouvez également exploiter les données sauvegardées sur la carte SD sur votre système PC via le lecteur de carte SD. Les données enregistrées sont affichées en fonction de leur extension et la date et l'heure sont comprises dans le nom de fichier.

16. Log de système

Cliquez sur ce lien dans l'écran de configuration pour afficher le fichier journal système. Ce fichier fournit des informations utiles sur la configuration et la connexion à l'issue du démarrage du système. La norme RFC 3164 est utilisée pour le fichier journal. Vous pouvez également envoyer des données à un serveur de fichiers journaux. Activez à cet effet l'option « Log à distance » et entrez l'adresse IP ainsi que le numéro de port du serveur.

17. Liste des paramètres

Cliquez sur ce lien dans l'écran de configuration pour afficher tous les paramètres système. Ces informations peuvent être mises à disposition en cas de demande d'assistance.

18. Gestion

Redémarrer

Redémarre le camera

Note: Quand vous choisissez mode duration, le camera redémarrais au 24h00 après N jour(s)

Redémarrer l'appareil

Mode duration :

Touts 1 [1~30] Jour(s)

Mode horaire :

Dim Lun Mar Mer Jeu Ven Sam

Heure 00:00 [hh:mm]

Sauvegarder Redémarrez maintenant

Sauvegarder Redémarrez maintenant

Restaurer

Restaurer tous les réglages aux réglages d'origine, sauf les réglages dans

Type de réseau Heure d'été

Restaurer

Exporter données

Exporter données de configuration de l'heure d'été file Exportation

Exporter réglage de la donnée de sauvegarde Exportation

Charger données

Actualiser règles heures d'été Durchsuchen... Chargement

Téléchargeur réglages donnée de sauvegarde Durchsuchen... Chargement

Actualiser logiciel

Sélectionner donnée du logiciel Durchsuchen...

Mise à jour

Redémarrer

Appuyez sur le bouton « Redémarrez maintenant » pour redémarrer le serveur vidéo. Vous pouvez également configurer un redémarrage automatique de l'appareil. Ceci peut s'avérer utile en cas de problèmes réseau. Nous vous conseillons de redémarrer le serveur vidéo une fois par semaine en cas de problèmes.

Restaurer
Appuyez sur le bouton « Restaurer » pour revenir aux réglages d'origine. Tous les réglages effectués sont alors effacés.

Exporter données
Appuyez sur le bouton « Exportation » pour exporter vos préréglages vidéo dans un fichier. Il est également possible d’exporter et de sauvegarder le fichier de configuration de l’heure d’été.

Charger données
Appuyez sur « Durchsuchen… » (Parcourir) et sélectionnez le fichier de configuration souhaité.
Appuyez ensuite sur « Chargement » et attendez que les réglages soient rétablis.

Actualiser logiciel
Vous pouvez ici accéder par Internet aux dernières mises à jour du logiciel du serveur vidéo avec l’assistant d’installation. Vous trouverez le logiciel à l’adresse suivante : www.abus-sc.com. Sélectionnez le fichier de mise à jour (*.pkg) et appuyez sur le bouton UPDATE. La mise à jour dure quelques instants. Le serveur vidéo est ensuite redémarré et fonctionne alors avec le nouveau logiciel.

Ne coupez en aucun cas l’alimentation électrique du serveur vidéo pendant une mise à jour de logiciel. Ceci pourrait entraîner des dommages irréversibles.
Une mise à jour de logiciel peut durer jusqu’à 10 minutes..

19. Maintenance et nettoyage

19.1 Test de fonctionnement

Contrôlez régulièrement la sécurité technique du produit, p. ex. endommagement du boîtier.

Si un fonctionnement en toute sécurité semble compromis, mettez le produit hors service et assurez-vous qu’il ne risque pas d’être mis en service accidentellement.

Un fonctionnement sûr peut être compromis quand :

- L’appareil présente des endommagements visibles,
- L’appareil ne fonctionne plus et
- après un stockage long dans de mauvaises conditions ou
- après avoir été soumis à de fortes contraintes lors du transport.

Vous n’avez pas à vous occuper de l’entretien du produit. Le produit ne contient aucun composant que vous deviez contrôler ou entretenir ; ne l’ouvrez jamais.

19.2 Nettoyage

Nettoyez le produit avec un tissu propre et sec. En cas d’encrassement important, le tissu peut être légèrement humidifié avec de l'eau tiède.

Empêchez tout liquide de pénétrer à l’intérieur de l’appareil ; ceci endommagerait l’appareil. N’utilisez pas de produits nettoyants chimiques ; cela risquerait d’endommager la surface du boîtier.

20. Elimination

Les appareils munis de ce symbole ne doivent pas être jetés dans les ordures ménagères. A la fin de sa durée de vie, éliminez le produit conformément aux dispositions légales en vigueur.
Veuillez vous adresser à votre vendeur ou éliminez les produits par le biais du point de collecte des déchets électroniques de votre commune.

21. Fiche technique

Numéro de type	**TVIP40000**
Type de caméra	Serveur vidéo
Résolution	QCIF,CIF,4CIF,D1 176 x 144 - 720 x 576 (étapes intermédiaires au choix)
Pixels (total)	720 x 576
Pixels (utiles)	720 x 576
Zoom numérique	x 4
Compression d'image	H.264, MPEG-4, MJPEG
Fréquence	H.264 720 X 480 à 30FPS, 720 x 576 à 25FPS
	MPEG-4 720 X 480 à 30FPS, 720 x 576 à 25FPS
	MJPEG 720 X 480 à 30FPS, 720 x 576 à 25FPS
Norme vidéo	PAL, NTSC
Nombre de flux parallèles	4
Nombre max. d'utilisateurs	10
Détection de mouvement	3 zones
Mémoire avant/après alarme	Oui
Superposition d'image	Date, nom de la caméra, zones privées
Entrée alarme (NO/NC)	1
Sortie à contact	1 (12 V c.c. à 400 mA)
Audio	Sortie audio (Speaker Out), entrée audio, audio 2 voies
Alerte	Notification par e-mail / FTP / HTTP / sortie relais / lecteur NAS /carte SD
Navigateurs pris en charge	Mozilla Firefox, Internet Explorer 6 ou une version supérieure
Logiciels pris en charge	Eytron VMS, assistance ONVIF
Carte SD	max. 32 GB (SD/SD-HC)
Port RS-485	Oui
Protocoles PTZ	Pelco D, Pelco P, LiLin, Samsung scc643, DynaDome / SmartDome
Connexion réseau	RJ-45 Ethernet 10/100 Base-T avec PoE
Protocoles réseau	IPv4, IPv6, TCP/IP, HTTP, UPnP, RTSP/RTP/RTCP, IGMP, SMTP, FTP, DHCP, NTP, DNS, CoS, QoS, SNMP, 802.1X
Cryptage	HTTPS SSLv3
Accès protégé	Filtre d'adresse IP, nom d'utilisateur, mot de passe, 3 niveaux d'autorisation
Alimentation électrique	12 V c.c. 24 V c.a. 802.3af PoE
Consommation de courant	max. 5,0 watts
Température de fonctionnement	0 °C à 55 °C
Dimensions (lxHxP)	75 x 35 x 150 mm
Certifications	CE, RoHS, C-Tick

22. Commandes URL

Les clients qui disposent déjà de leur propre site web ou application de contrôle web peuvent y intégrer facilement la serveur vidéo réseau ou le serveur vidéo par syntaxe URL. Cette section définit l'interface de programmation d'application HTTP externe. Pour une liste complète des commandes URL, veuillez vous reporter à l'annexe.

23. Informations relatives aux licences

Il est à noter que le serveur vidéo réseau TVIP40000 intègrent notamment du code source Linux dont la licence est gérée suivant le principe GNU General Public Licence (GPL). Pour assurer un usage conforme au principe de la licence GPL du code source utilisé, nous vous renvoyons aux conditions de licence GPL.

Texte de la licence

Le texte de la licence GNU General Public Licence se trouve sur le CD des logiciels fourni avec votre produit, ainsi que sur le site d'ABUS Security-Center à l'adresse http://www.abus-sc.de/DE/Service-Downloads/Software?q=GPL.

Code source

Le code source utilisé est disponible sur le site d'ABUS Security-Center à l'adresse http://www.abus-sc.de/DE/Service-Downloads/Software?q=GPL
où il peut être téléchargé librement.

Fonctionnement du système

Le téléchargement des paquetages (codes source) ne permet pas la constitution d'un système opérationnel. D'autres logiciels sont nécessaires, outre le matériel que représente la serveur vidéo réseau.

24. Avis concernant les licences technologiques

Technologie H.264, MPEG-4 AAC

CE PRODUIT EST CONCÉDÉ SELON LES CONDITIONS DE LA LICENCE DE BREVET H.264, MPEG-4 AAC AUDIO. IL NE DOIT FAIRE L'OBJET D'AUCUNE DÉCOMPILATION, INGÉNIERIE INVERSE OU COPIE, À L'EXCEPTION DE LA COPIE UNIQUE AUTORISÉE À DES FINS D'ARCHIVAGE POUR LES LOGICIELS INFORMATIQUES. POUR PLUS D'INFORMATIONS, VEUILLEZ CONSULTER LE SITE HTTP://WWW.VIALICENSING.COM.

Technologie H.264, MPEG-4 Visual

CE PRODUIT EST CONCÉDÉ SELON LES CONDITIONS DE LA LICENCE DE PORTEFEUILLE DE BREVETS H.264, MPEG-4 VISUAL DANS LE CADRE DE L'UTILISATION PERSONNELLE ET NON COMMERCIALE D'UN CONSOMMATEUR EN VUE (i) DE L'ENCODAGE VIDÉO CONFORMÉMENT À LA NORME MPEG-4 VISUAL (« MPEG-4 VIDEO ») ET/OU (ii) DU DÉCODAGE DE CONTENU MPEG-4 VIDEO QUI A ÉTÉ ENCODÉ PAR UN CONSOMMATEUR ENGAGÉ DANS UNE ACTIVITÉ PERSONNELLE ET NON COMMERCIALE ET/OU A ÉTÉ OBTENU AUPRÈS D'UN FOURNISSEUR VIDÉO AUTORISÉ PAR MPEG LA À FOURNIR DU CONTENU MPEG-4 VIDEO. AUCUNE LICENCE N'EST ACCORDÉE DE MANIÈRE EXPLICITE OU IMPLICITE POUR AUCUN AUTRE USAGE. POUR DE PLUS AMPLES

INFORMATIONS, Y COMPRIS AU SUJET DES UTILISATIONS ET DES LICENCES PROMOTIONNELLES, INTERNES ET COMMERCIALES, VEUILLEZ VOUS ADRESSER À MPEG LA, LLC. VOIR HTTP://WWW.MPEGLA.COM.

Norme AMR-NB

CE PRODUIT EST CONCÉDÉ SELON LES CONDITIONS DE LA LICENCE DE BREVET DE LA NORME AMR-NB. L'UTILISATION DE CE PRODUIT PEUT ÊTRE SOUMISE À L'APPLICATION DES BREVETS DES CONCÉDANTS DE LICENCE SUIVANTS :
TELEFONAKIEBOLAGET ERICSSON AB : US PAT. 6192335; 6275798; 6029125; 6424938; 6058359. NOKIA CORPORATION : US PAT. 5946651; 6199035. VOICEAGE CORPORATION : AT PAT. 0516621; BE PAT. 0516621; CA PAT. 2010830; CH PAT. 0516621; DE PAT. 0516621; DK PAT. 0516621; ES PAT. 0516621; FR PAT. 0516621; GB PAT. 0516621; GR PAT. 0516621; IT PAT. 0516621; LI PAT. 0516621; LU PAT. 0516621; NL PAT. 0516621; SE PAT 0516621; US PAT 5444816; AT PAT. 819303/AT E 198805T1; AU PAT. 697256; BE PAT. 819303; BR PAT. 9604838-7; CA PAT. 2216315; CH PAT. 819303; CN PAT. ZL96193827.7; DE PAT. 819303/DE69611607T2; DK PAT. 819303; ES PAT. 819303; EP PAT. 819303; FR PAT. 819303; GB PAT. 819303; IT PAT. 819303; JP PAT. APP. 8-529817; NL PAT. 819303; SE PAT. 819303; US PAT. 5664053. CETTE LISTE PEUT ÊTRE MISE À JOUR À TOUT MOMENT PAR LES CONCÉDANTS DE LICENCE. LA VERSION LA PLUS RÉCENTE DE CETTE LISTE EST DISPONIBLE SUR LE SITE WEB DES CONCÉDANTS DE LICENCE À L'ADRESSE HTTP://WWW.VOICEAGE.COM.

ABUS
Security Tech Germany

eyseo.ip

TVIP40000

Gebruiksaanwijzing

Versie 10/2010

Originele Engelstalige handleiding. Bewaren om eventueel later te raadplegen.

Introductie

Geachte klant,

hartelijk dank voor de aanschaf van dit product.

**Dit product voldoet aan alle geldende Europese en landelijke voorschriften. De bijbehorende documentatie is op verzoek bij de fabrikant beschikbaar.
(www.abus-sc.com).**

Om aan deze voorwaarden te blijven voldoen en werking zonder gevaar te garanderen, moet u als gebruiker deze bedieningshandleiding in acht nemen!

Voordat u dit apparaat voor de eerste keer in gebruik neemt, moet u de handleiding volledig lezen en de bijbehorende veiligheidsinstructies in acht nemen.

Bij vragen kunt u contact opnemen met uw leverancier!

Disclaimer

Deze handleiding is met de grootste zorg samengesteld. Wanneer u desondanks van mening bent dat er informatie ontbreekt of dat er onjuistheden voorkomen, kunt u contact opnemen met het adres achter in deze handleiding.
ABUS Security-Center GmbH aanvaardt geen aansprakelijkheid voor technische fouten en drukfouten en behoudt zich het recht voor om op elk moment zonder voorafgaande aankondiging wijzigingen aan te brengen in het product of deze handleiding. De fabrikant aanvaardt geen aansprakelijkheid voor directe of indirecte schade die ontstaat op grond van uitvoering, prestaties en gebruik van dit product.
Er bestaat geen garantie op de juistheid van de informatie in deze handleiding.

Uitleg van de symbolen

Een bliksemschicht in een driehoek geeft een gevaar voor de gezondheid aan, bv. gevaar voor een elektrische schok.

Een uitroepteken in de driehoek wijst in deze handleiding op een belangrijke opmerking die in acht moet worden genomen.

Dit symbool vindt u bij de tips en informatie over gebruik en bediening.

Belangrijke veiligheidswaarschuwing

In geval van schade als gevolg van het niet in acht nemen van deze bedieningsinstructies komt de garantie te vervallen. ABUS is niet aansprakelijk voor eventuele gevolgschade!

ABUS aanvaardt geen aansprakelijkheid voor persoonlijk letsel of schade aan eigendommen voor zover deze het gevolg is van onjuiste handelingen of het niet in acht nemen van de veiligheidsinstructies.
In dergelijke gevallen komt de garantie te vervallen.

Geachte klant,
De onderstaande veiligheidsinstructies zijn niet alleen bedoeld ter bescherming van uw veiligheid en gezondheid, maar ook ter bescherming van het apparaat. Lees de onderstaande punten s.v.p. aandachtig door.

- In dit product bevinden zich geen onderdelen die onderhoud nodig hebben. Afgezien hiervan, vervallen de (CE) goedkeuring en de garantie wanneer u dit product opent of uit elkaar haalt.
- Het product kan bij een val, zelfs van geringe hoogte, worden beschadigd.
- Dit apparaat kan alleen binnenshuis worden gebruikt.
- Let er bij installatie op dat er geen direct zonlicht op de beeldsensor kan vallen. Neem s.v.p. de installatie-instructies in het bijbehorende hoofdstuk van deze handleiding in acht.

Gebruik het apparaat niet in de volgende ongunstige omstandigheden:

- Vocht of hoge luchtvochtigheid
- Extreem hoge of lage temperatuur
- Direct zonlicht
- Omgeving met stof of explosieve gassen, dampen of oplosmiddelen
- Sterke vibraties
- Sterke magnetische velden die bv. voorkomenin de omgeving van machines of luidsprekers
- De videoserver mag niet op een onstabiel oppervlak worden aangebracht.

Algemene veiligheidsinstructies:

- Laat geen verpakkingsmateriaal zonder toezicht liggen. Plastic folie/zakken, polystyreen verpakkingsmateriaal etc. kunnen gevaarlijk speelgoed vormen voor kinderen.
- De videoserver bevat kleine onderdelen die kunnen worden ingeslikt en mag daarom om veiligheidsredenen niet in handen komen van kinderen.
- Steek niets door de openingen in het apparaat.
- Maak uitsluitend gebruik van accessoires die door de fabrikant worden geadviseerd. Sluit geen incompatibele componenten op het apparaat aan.
- Neem de veiligheidsinstructies en handleidingen van de overige aangesloten apparatuur in acht.
- Controleer het apparaat vóór installatie op beschadigingen. Het apparaat mag niet worden gebruikt wanneer er beschadigingen worden vastgesteld.
- Neem s.v.p. de opgaven met betrekking tot de bedrijfsspanning in de technische gegevens in acht. Te hoge spanning kan het apparaat vernielen en kan gevaar voor elektrische schok opleveren.

Veiligheidswaarschuwing

1. Voedingsspanning: netvoeding 110 - 250 VAC, 50/60 Hz / 12 VDC, 1,5 A (in de verpakking meegeleverd.)
   Gebruik dit apparaat uitsluitend met het type netvoeding dat op het etiket is aangegeven. Wanneer u niet zeker bent van de netspanning die aan uw woning wordt geleverd, kunt u contact opnemen met uw plaatselijke energieleverancier. Koppel het apparaat los van het lichtnet voordat u onderhouds- of installatiewerkzaamheden uitvoert.

2. Overbelasting
   Voorkom overbelasting van een stopcontact, verlengkabel of adapter. Door overbelasting kan brand of een elektrische schok worden veroorzaakt.

3. Reiniging
   Koppel het apparaat vóór reiniging los van het lichtnet. Gebruik een vochtige doek (geen oplosmiddelen) om stof van het apparaat te verwijderen.

Waarschuwingen

Neem alle veiligheids- en bedieningsinstructies in acht voordat u het apparaat inschakelt!

1. Neem de volgende aanwijzingen in acht om beschadigingen aan de stekker of de kabel te vermijden:
   - Breng geen wijzigingen aan in de stekker of de kabel.
   - Buig of draai de kabel niet.
   - Verbreek de verbinding met het lichtnet door de stekker vast te houden. Trek de stekker niet aan de kabel uit het stopcontact.
   - Houd verwarmingsbronnen zo ver mogelijk uit de buurt van de netkabel om smelten van de vinylmantel te voorkomen.

2. Neem deze aanwijzingen in acht. Niet in acht nemen van één of alle aanwijzingen kan een elektrische schok veroorzaken.
   - De behuizing mag uitsluitend worden geopend voor het plaatsen van een harde schijf. Koppel dit apparaat los van het lichtnet voordat u hiermee begint.
   - Plaats geen metalen of brandbare voorwerpen in het apparaat.
   - Maak tijdens onweer gebruik van een bliksembeveiliging om schade te voorkomen.

3. Gebruik het apparaat niet wanneer het gebreken vertoont. Er kan ernstige schade ontstaan wanneer u een defect apparaat blijft gebruiken. Neem contact op met uw leverancier wanneer het apparaat defect is.

Bij installatie in een bestaand videobewakingssysteem dient u er voor te zorgen dat alle apparatuur is losgekoppeld van het lichtnet en de laagspanningsvoedingen.

Bij twijfel wordt geadviseerd om de installatie en de aanleg van de bedrading te laten uitvoeren door een vakkundige elektricien. Onjuiste elektrische aansluitingen op het lichtnet vormen niet alleen een gevaar voor u maar ook voor anderen.
Zorg er bij het aansluiten van het volledige systeem voor dat het lichtnet en het laagspanningscircuit gescheiden blijven en tijdens normaal gebruik of bij storing niet met elkaar in contact kunnen komen.

Uitpakken

Behandel het apparaat tijdens het uitpakken met de grootst mogelijke voorzichtigheid.

Controleer het apparaat direct wanneer u beschadigingen aan de verpakking vaststelt.
Neem contact op met uw leverancier wanneer het apparaat beschadigd is.

Inhaltsverzeichnis

Bedoeld gebruik

Een uitvoerige functiebeschrijving vindt u in hoofdstuk „4. Eerste ingebruikneming”.

Elk ander gebruik dan hetgeen hierboven is beschreven kan leiden tot beschadiging van het product en andere gevaren veroorzaken. Bij gebruik voor andere toepassingen zal de garantie en elke vorm van aansprakelijkheid vervallen. Dit zal ook het geval zijn wanneer er ongeoorloofde wijzigingen of aanpassingen aan het product worden gemaakt.

Lees s.v.p. deze handleiding volledig en zorgvuldig door voordat u dit apparaat in gebruik neemt. Deze handleiding bevat richtlijnen die van belang zijn voor correcte bevestiging en gebruik.

1. Leveringsomvang

D1 netwerk videoserver
TVIP40000

Netvoeding

Houder

Korte handleiding

Software CD
met gebruikershandleiding

2. Installatie

Controleer of alle hierboven genoemde accessoires aanwezig zijn. Voor gebruik van deze videoserver is een Ethernet netwerkkabel benodigd. Deze kabel moet voldoen aan de UTP specificatie categorie 5 (CAT5) en mag niet langer zijn dan 100 meter.

2.1 Voeding

Controleer voordat u met de installatie begint of de netspanning en de nominale spanning van de videoserver overeenkomen.

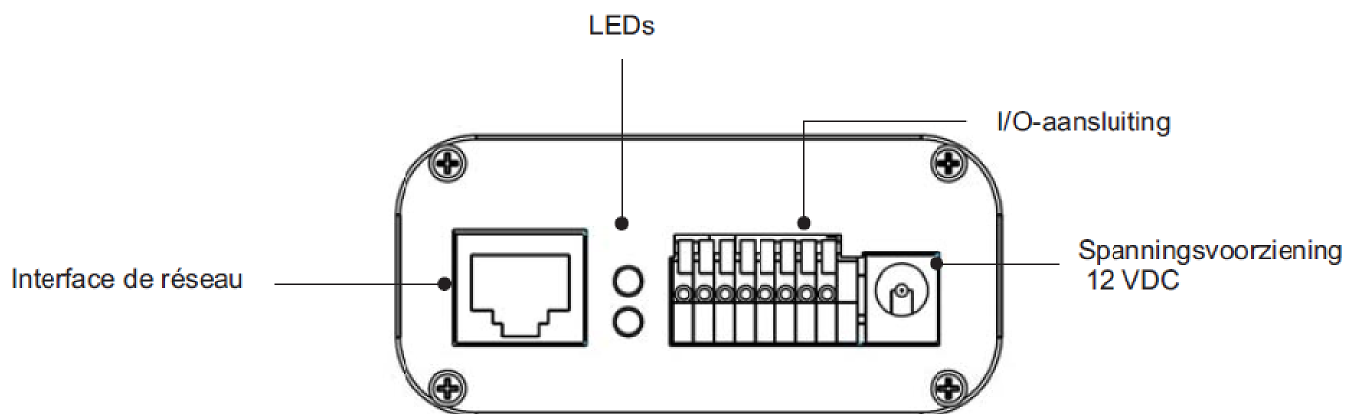
2.2 Bevestigen van de videoserver

Voor de wandmontage van de videoserver zijn de in de leveringsomvang voorhanden klembeugels en schroeven nodig.

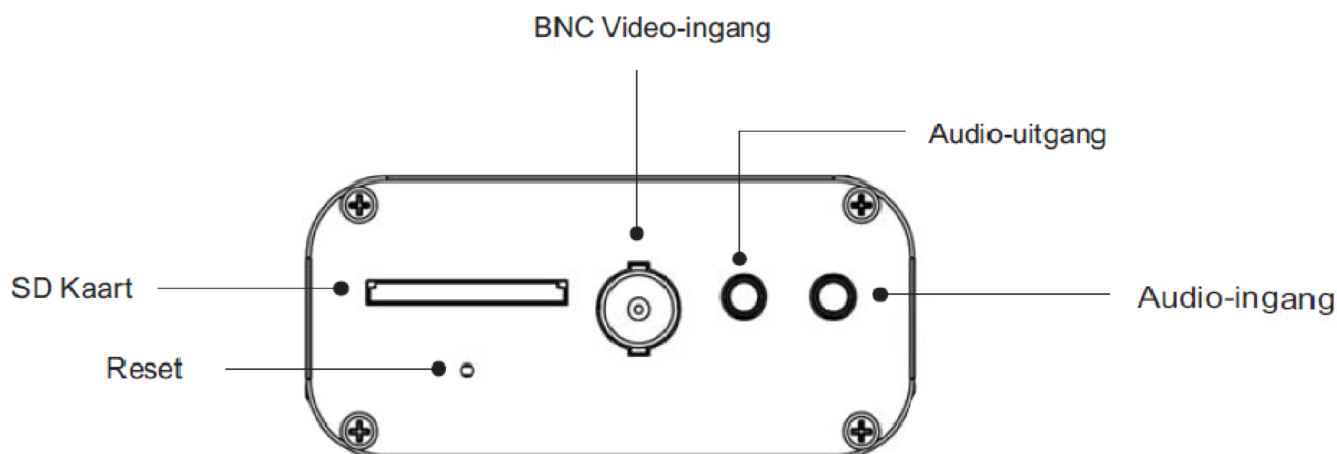
LET OP!
Zorg er voor dat de voedingsspanning van de videoserver tijdens de installatie is losgekoppeld.

3. Beschrijving van de videoserver

3.1 Vooraanzicht

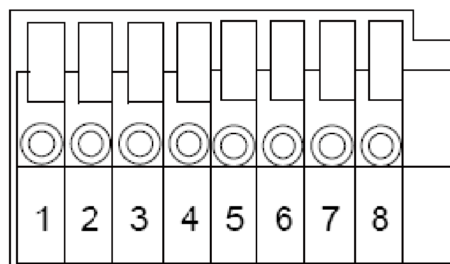


3.2 Achteraanzicht

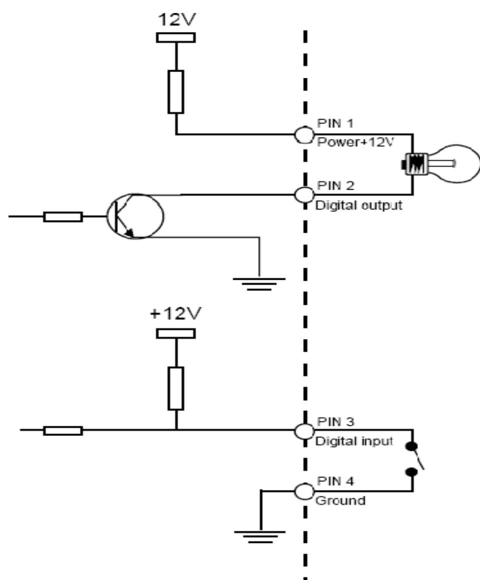


3.3 Alarmingangen en digitale uitgangen

PIN	Beschrijving
1	+12V uitgang
2	Digitale uitgang
3	Digitale ingang
4	Massa
5	24V AC ingang
6	24V AC ingang
7	RS-485 +
8	RS-485 -



3.4 Gate ingang / uitgang en status display



Beschrijving status LED

Status / LED kleur	Groen	Rood
Systeem start	Uit	Aan
Videoserver uitgeschakeld	Uit	Uit
Netwerk OK	1/s	Aan
Netwerkprobleem	Uit	Aan
Firmware update	1/s	0,1/s
Fabrieksinstellingen herstellen	0,1/s	0,1/s

Druk op de **resetknop** om de videoserver te herstarten of de fabrieksinstellingen te herstellen. Gebruik hiervoor een passend (klein) gereedschap.

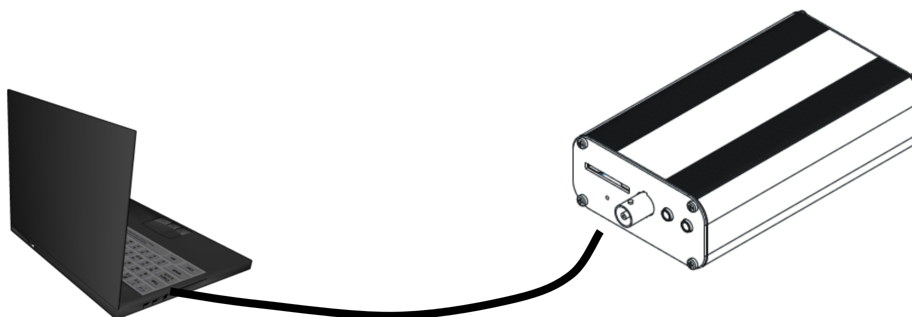
Videoserver herstarten: druk eenmaal op de resetknop en wacht tot de videoserver opnieuw opstart.

Herstellen van de fabrieksinstellingen: houd de resetknop gedurende ca. 30 seconden ingedrukt tot de status LED begint te knipperen. Alle instellingen zullen worden hersteld naar de standaard fabrieksinstellingen.

4. Eerste keer opstarten

Directe verbinding tussen de videoserver en de PC / notebook

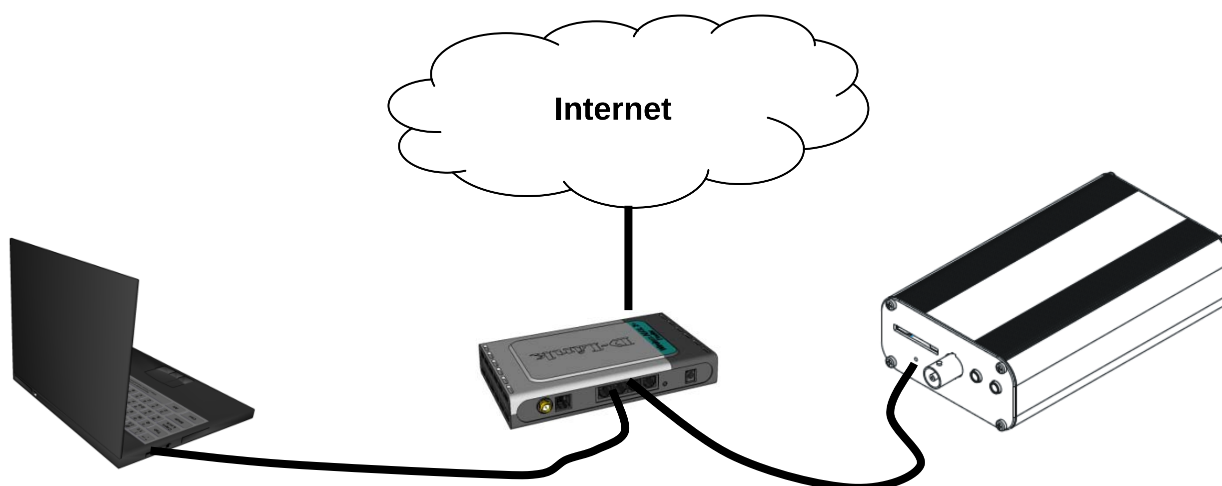
1. Maak hiervoor gebruik van een zgn. gekruiste („crosslink”) netwerkkabel.
2. Sluit de kabel aan tussen de Ethernet aansluiting van de PC / notebook en de netwerkvideoserver.
3. Sluit de netvoeding van de netwerkvideoserver aan.
4. Zet het IP-adres van de PC / notebook op 169.254.0.1.
5. Ga verder met punt 5.1 om de initiële installatie af te ronden en verbinding te maken met de videoserver.



➀ Gekruiste of "crosslink" Ethernet kabel

De videoserver aansluiten via een router / switch

1. Maak gebruik van een set patchkabels.
2. Sluit een van de kabels aan tussen de Ethernet aansluiting van de PC / notebook en de router / switch.
3. Sluit de andere kabel aan tussen de videoserver en de router / switch.
4. Sluit de netvoeding van de netwerkvideoserver aan.
5. Wanneer er een DHCP server op het netwerk actief is: zet het IP-adres van de PC / notebook op "automatisch IP-adres ontvangen".
   Wanneer er geen DHCP server op het netwerk actief is: zet het IP-adres van de PC / notebook op 169.254.0.1.
6. Ga verder met punt 5.1 om de initiële installatie af te ronden en verbinding te maken met de videoserver.



4.1 Eerste netwerktoegang naar de videoserver

De eerste keer via het netwerk verbinding maken met de videoserver gebeurt met het programma "Installatieassistent 2".
Wanneer de assistent wordt gestart, wordt er automatisch gezocht naar alle aangesloten eyseo.ip netwerkvideoserver's en videoservers.

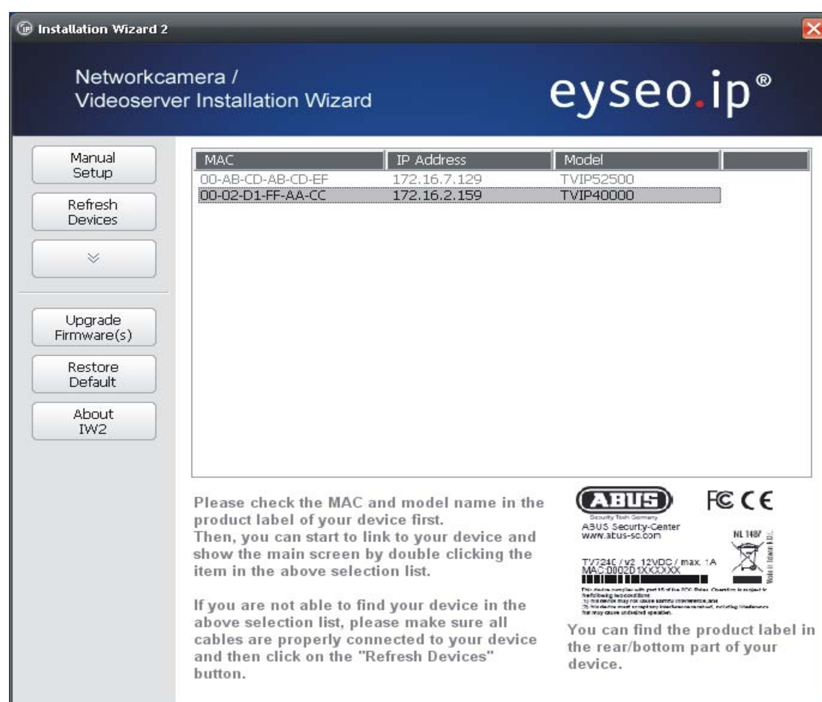
U vindt dit programma op de CD onder **CD-ROM\Tools\EyseoIP Tools**

Installeer het programma op uw PC en start het. De assistent zal automatisch uw netwerk afzoeken naar eyseo.ip netwerkvideoserver's.

De fabrieksinstelling voor het IP-adres is **169.254.0.99**. Zonder installatieassistent kan de videoserver alleen worden verbonden wanneer het IP-adres van de PC tussen 169.254.0.1 en 169.254.0.98 is ingesteld.

Wanneer er een DHCP server op het netwerk actief is, zal het IP-adres voor de PC en de videoserver automatisch worden toegewezen.

Start nu de installatieassistent. Wanneer er geen DHCP server actief is, voegt de installatieassistent een virtueel IP-adres toe in het bereik 169.1254.0.xx. Zolang de installatieassistent actief is, kunt u de via het virtuele IP-adres verbinding maken met de videoserver. Wij adviseren om de netwerkinstellingen van de videoserver direct aan te passen aan de IP instellingen van het PC netwerk.



Nadat de installatieassistent 2 is afgesloten zal het virtuele IP-adres worden verwijderd. Wanneer het IP-aders van de videoserver zich nog in een ander bereik bevindt dan het PC netwerk, is er gen toegang tot de netwerkvideoserver meer mogelijk.

4.2 Via een browser verbinding maken met de netwerkvideoserver

Wanneer u verbinding maakt via Mozilla Firefox of Netscape zal er een QuickTime stream worden weergegeven. Hiervoor moet het programma QuickTime van Apple zijn geïnstalleerd.

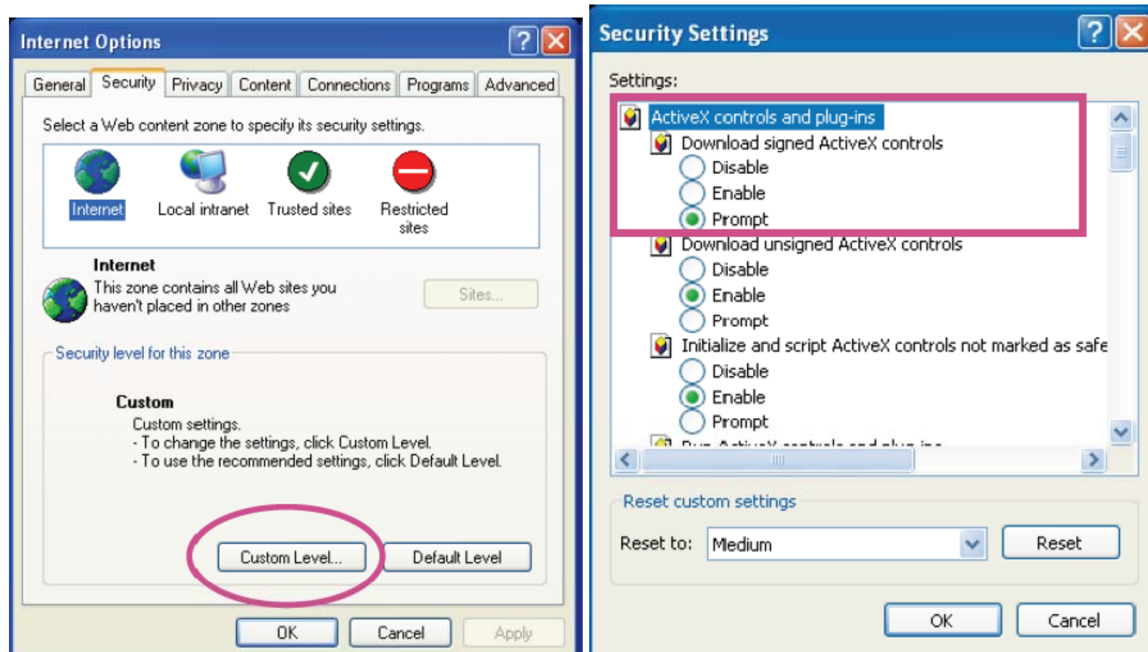
Om de videostream weer te geven met Microsoft Internet Explorer is er een video invoegtoepassing benodigd. Deze zal worden geïnstalleerd wanneer er verbinding wordt gemaakt met de netwerkvideoserver. Er zal een venster verschijnen met de vraag of u de invoegtoepassing wilt installeren. Druk op de knop "Installeren" om de invoegtoepassing te installeren. Afhankelijk van de beveiligingsinstelling van Internet

Explorer is het mogelijk dat de installatie wordt geblokkeerd. In dit geval moet u de beveiligingsinstellingen aanpassen.

4.3 Installatie van de Active-X invoegtoepassing

Bij Mozilla Firefox of Netscape gebruikers zal de browser gebruikmaken van QuickTime om de livevideo te streamen. Wanneer u QuickTime niet op uw computer heeft geïnstalleerd, moet u het eerst downloaden, start vervolgens uw webbrowser.

4.4 Aanpassen van de beveiligingsinstellingen



OPMERKING!
De beveiligingsinstellingen van Internet Explorer kan de weergave van de videostream blokkeren. Wijzig de instellingen via "Extras/Internet opties /Beveiliging" naar een lager niveau. Zorg er voor dat ActiveX besturingselementen op een aangepast niveau worden geactiveerd.

4.5 Identificatie met een wachtwoord

In de fabriek is er geen beheerderswachtwoord ingesteld voor toegang tot de videoserver. Om veiligheidsredenen moet de beheerder direct na de installatie een wachtwoord aanmaken. Nadat er een

beheerderswachtwoord is ingesteld, zal de videoserver bij elke toegang vragen naar een gebruikersnaam en een wachtwoord.

De permanente standaard gebruikersnaam voor de beheerder is **"root"**. Dit kan niet worden gewijzigd. Een vergeten wachtwoord kan alleen worden hersteld door de fabrieksinstellingen van de videoserver te herstellen.

Voor toegang tot de videoserver moet de gebruikersnaam "root" en het hierboven ingestelde wachtwoord worden ingevoerd.

➔ Na correcte identificatie zal er een verbinding worden gemaakt met de videoserver en zal de videostream worden weergegeven.

4.6 Via een RTSP speler verbinding maken met de netwerkvideoserver

De MPEG-4 videostream kan worden weergegeven door verbinding met de videoserver te maken via een RTSP compatibele mediaspeler. De volgende gratis mediaspelers ondersteunen RTSP:

- VLC Media Player
- Real Player
- QuickTime Media Player

Het RTSP adres moet als volgt worden ingevoerd:

rtsp://<IP-adres van de netwerkvideoserver>:<rtsp Port>/<naam van de videostream>

Verderop in deze handleiding wordt uitgelegd hoe u de naam van de videostream kunt veranderen.

Voorbeeld:
rtsp://192.168.0.99:554/live.sdp

4.7 Via een mobiele telefoon verbinding maken met de netwerkvideoserver

Zorg er voor dat uw telefoon in staat is om een verbinding met internet te maken. Bovendien moet de mobiele telefoon zijn voorzien van een RTSP compatibele mediaspeler zoals:

- Real Player
- Core Player

Meer informatie vindt u in het hoofdstuk "RTSP-verbinding".

Let er op dat beperkte toegang mogelijk is in verband met de beperkte bandbreedte van het mobiele netwerk. Wij adviseren de volgende instellingen om de videostream te optimaliseren:

Videocompressie	MPEG-4
Resolutie	176 x 144
I Frame	1 seconde
Videokwaliteit (constante bitrate)	40 Kbit / sec.
Audio compressie (GSM-AMR)	12.2 Kbit / sec.

Wanneer de mediaspeler geen RTSP authenticatie ondersteunt, moet u deze optie bij de RTSP instellingen van de netwerkvideoserver uitschakelen.

Het RTSP adres moet als volgt worden ingevoerd:

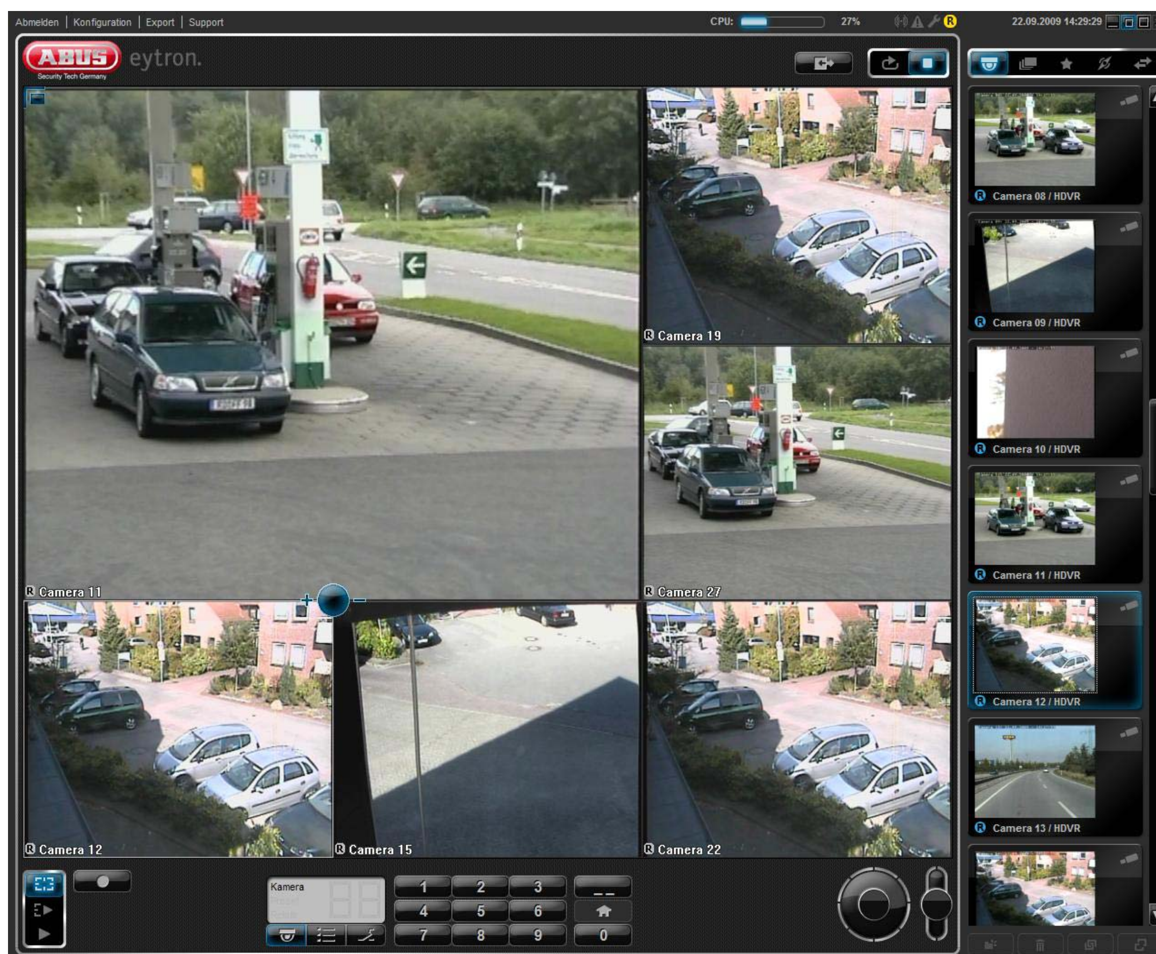
rtsp://<IP-adres van de netwerkvideoserver>:<rtsp Port>/<naam van de videostream>

Verderop in deze handleiding wordt uitgelegd hoe u de naam van de videostream kunt veranderen.

Voorbeeld:
rtsp://192.168.0.99:554/live.sdp

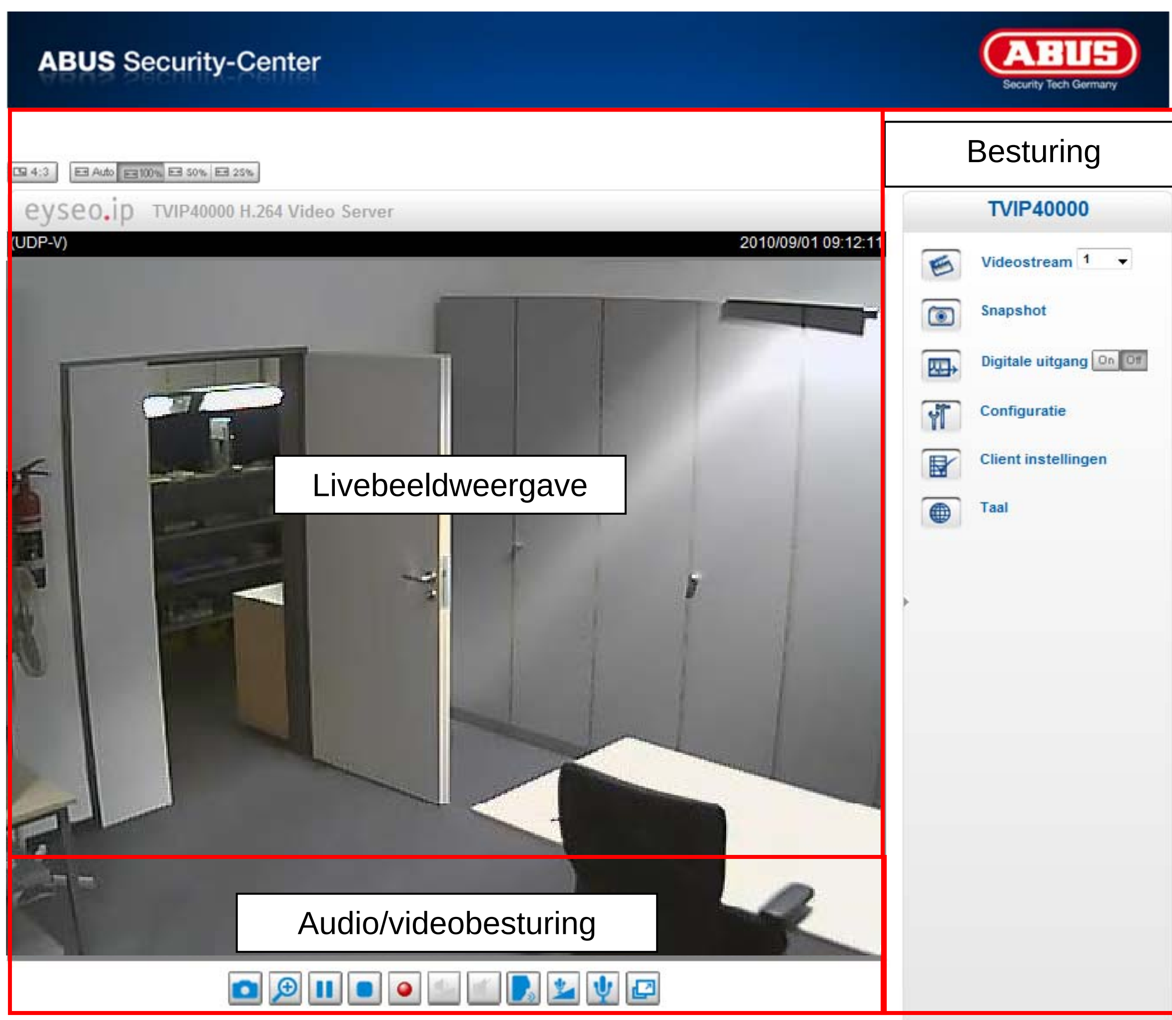
4.8 Via eytron VMS Express verbinding maken met de netwerkvideoserver

De meegeleverde CD bevat de gratis eytron VMS Express opnamesoftware. Met deze software is het mogelijk om verschillende IP videoserver's weer te geven en op te nemen. Verdere informatie vindt u in de handleiding van de software op de CD.



5. Gebruikersfuncties

Open de startpagina van de videoserver. De interface is in de volgende hoofdbereiken onderverdeeld:



Livebeeldweergave

- Verander de zoomstand door het bedienen van het muisscrollwiel
- Door een klik in het livebeeld kunt u direct de besturing van een analoge draai/kantelcamera overnemen.

Videoserverbesturing

Videostream

Kies tussen videostream 1-4 voor de livebeeldweergave

Momentopname

Maak een momentopname (zonder ActiveX-Plugin)

Schakeluitgang

Schakeluitgang handmatig in- en uitschakelen

Configuratie

Videoserverconfiguratie uitvoeren (administratorinstellingen)

Klantinstellingen

Klantinstellingen invoeren. Details vindt u op de volgende pagina's

Taal

Taalinstelling van de interface aanpassen

PTZ-besturing

Gebruik de stuurknoppen voor digitale en mechanische PTZ-functie

Aangepaste venstergrootte

Hiermee kan het livebeeld in 3 verschillende zoomstanden (100%, 50% en 25%) aangepast worden. Het is ook mogelijk om het livebeeld automatisch aan het actuele browserformaat aan te passen. Hiervoor moet de optie „AUTO" gekozen worden.

Beeldschermverhouding

Met de knop „4:3" wordt de paginaverhouding van het livebeeld op 4:3 vastgelegd.

Menu in-/uitklappen

Met deze functie kan de menubesturing in- en uitgeklapt worden.

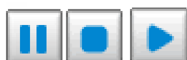
5.1 Audio/videobesturing

Momentopname

De webbrowser geeft een nieuw venster aan waarin de momentopname getoond wordt. Om het beeldbestand op uw pc op te slaan, klikt u met de rechter muisknop op het beeldvlak en kiest u de optie „Opslaan als".

Digitale zoom en momentopname

Klik op het vergrootglassymbool onder het videoserveraanzicht. Daarna verschijnt het bedieningsveld voor de digitale zoom. Deactiveer het controleveld „Digitale zoom deactiveren" en wijzig de zoomfactor met de schuifregelaar.

 Start/stop van de livebeeldweergave

De livestream kan naar keuze gestopt of beëindigd worden. In beide gevallen kan met het playsymbool de livestream voortgezet worden.

Lokale opname

Er kan een opname op de lokale harde schijf gestart of gestopt worden. Het opnamepad wordt onder „Klantinstellingen" geconfigureerd.

Volume aanpassen

Klik op het symbool om handmatig het niveau voor de audio-uitgang in te stellen.

Audio aan/uit

Spreken

Zolang de knop ingedrukt is, worden audiosignalen van de pc aan de audio-uitgang van de videoserver overgedragen.

Microfoonvolume

Klik op het symbool om handmatig het niveau voor de audio-ingang van de videoserver aan te passen.

Mute

Schakel de audio-ingang van de videoserver in/uit.

Volledig beeld

Activeer het aanzicht volledig beeld. Het livebeeld van de videoserver wordt beeldschermvullend weergegeven.

5.2 Klantinstellingen

De gebruikersinstellingen worden op de lokale computer opgeslagen. De volgende instellingen staan ter beschikking:

Mediaopties maakt het de gebruiker mogelijk om de audio- of videofuncties te deactiveren.

Protocolopties maakt de keuze van een verbindingsprotocol tussen de client en de server mogelijk. Twee protocolopties staan voor de optimalisatie van de toepassing ter beschikking: UDP, TCP, HTTP.

Het UDP-protocol maakt een groter aantal realtime audio- en videostreams mogelijk. Sommige datapakketten kunnen hierbij echter wegens een grote hoeveelheid data in het netwerk verloren gaan. Beelden kunnen hierdoor alleen onduidelijk weergegeven worden. Het UDP-protocol wordt aanbevolen als geen speciale eisen gesteld worden.

In het TCP-protocol gaan minder datapakketten verloren en een preciezere videoweergave wordt gegarandeerd. Het nadeel van dit protocol bestaat echter daarin dat de realtime stream slechter is dan deze van het UDP-protocol

Het HTTP-protocol kiest u als het netwerk door een firewall beschermd en alleen de HTTP-poort (80) geopend moet worden.

De keuze van het protocol wordt in de volgende volgorde aanbevolen: UDP – TCP – HTTP

MP4 opnameopties: maakt het de gebruiker mogelijk om het bestandspad voor de directe gegevensopslag aan te passen. De knop „Datum en tijd aan bestandsnaam hangen" creëert bestanden met de volgende identificatie:

CLIP_20091115-164403.MP4
Bestandsnaam-aanvulling_JaarMaandDag-UurMinuutSeconde.MP4

MP4 opslagopties

Map: c:\recordings Bladeren...

Bestandsnaam voorvoegsel: CLIP

☑ Tijd en datum toevoegen aan de bestandsnaam

Opslaan

De opgenomen gegevens kunnen via een MP4-compatiebele videospeler weergegeven worden (bijv. VLC Mediaplayer).

6. Administratorinstellingen

6.1 Systeem

Alleen de administrator heeft toegang tot de systeemconfiguratie. Elke categorie in de linkerkolom wordt op de volgende pagina's verklaard. De vetgedrukte teksten vormen de specifieke gegevens op de optiepagina's. De administrator kan de URL onder de afbeeldingen invoeren om direct naar de beeldpagina van de configuratie te gaan.

ABUS Security-Center
ABUS Security Tech Germany

Configuratie
- Systeem
- Veiligheid
- HTTPS
- SNMP
- Netwerk
- DDNS
- Toegangslijst
- Audio en video
- Bewegingsdetectie
- Camera manipulatiedetectie
- Camerabesturing
- Toepassing
- Opname
- Lokale opslag
- Systeemlog
- Parameters weergeven
- Onderhoud

Version: 1210l

Home

Systeem
Hostnaam: TVIP40000 H.264 Video Server
☐ LED indicator uitschakelen

Systeemtijd
Tijdzone: GMT+01:00 Amsterdam, Berlijn, Rome, Stockholm, Wenen, Madrid, Parijs
☐ Zomertijd inschakelen:

Let op: Je kunt je Daylight Time inzake het onderhoud pagina opslaan of gebruik de camera standaard waarde.

◉ Huidige tijd en datum behouden
○ Synchroniseren met de computertijd
○ Handmatig
○ Automatisch

Di en Do
Digitale ingang: actieve status is Laag ; De huidige status is **Hoog**
Digitale uitgang: actieve status is Geaard ; De huidige status is **Open**

Opslaan

„Hostnaam” De tekst geeft de titel op de hoofdpagina weer.

„LED-weergave uitschakelen” Kies deze optie om de LED-weergave van de videoserver uit te schakelen. Hiermee kan verhinderd worden dat andere personen de werking van de videoserver kunnen vaststellen.

„Tijdzone” Past de tijd volgens de gekozen tijdzone aan.

„Zomertijd activeren” Activeert de zomertijdinstellingen in de videoserver. Alle zomertijdinstellingen voor elke tijdzone zijn al in de videoserver opgeslagen.

„Actuele vermelding van datum en tijd behouden” Klik op deze optie om de actuele datum en tijd van de videoserver te behouden. Met een interne realtimeklok blijven de datum en de tijd van de videoserver zelfs na een spanningverlies behouden.

„Pc-tijd overnemen” Synchroniseert de datum en de tijd van de videoserver met de lokale computer. De schrijfbeveiligde datum en de schrijfbeveiligde tijd van de pc worden na actualisering weergegeven.

„Handmatig” Stelt de datum en de tijd afhankelijk van de invoer door de administrator in. Neem bij het invoeren het formaat in het betreffende veld in acht.

„Automatisch” Synchroniseert datum en tijd met de NTP-server via het internet telkens bij het starten van de videoserver. Dit zal niet lukken als de toegewezen tijdserver niet bereikbaar is.

„NTP-server” Wijst het IP-adres of de domeinbenaming van de tijdserver toe. Door het leeg laten van dit tekstvakje wordt de videoserver met de standaard tijdservers verbonden.

„DI en DO” Stelt de voorgedefinieerde toestand voor alarmingang en relaisuitgang in.

Vergeet niet op **„Opslaan”** te klikken opdat de wijzigingen actief worden.

6.2 Veiligheid

„Rootpaswoord” Dient voor het wijzigen van het administratorpaswoord door het invoeren van het nieuwe paswoord. De ingevoerde paswoorden worden om veiligheidsredenen alleen met punten weergegeven. Na het klikken op **„Opslaan”** vraagt de webbrowser de administrator om het nieuwe paswoord voor de toegang tot de videoserver in te voeren.

„Gebruiker toevoegen” Voer de nieuwe gebruikersnaam en het bijbehorende paswoord in en klik daarna op **„Toevoegen”**. De nieuwe gebruiker wordt op de lijst met de gebruikersnamen weergegeven. In het totaal kunnen twintig gebruikersaccounts ingesteld worden.

„Gebruiker bewerken” Open de lijst met de gebruikersnamen, zoek de gebruiker die u wilt bewerken en verander de betreffende waarden. Klik op **„Actualiseren”** om de wijzigingen over te nemen.

„Gebruiker wissen" Open de lijst met de gebruikersnamen, zoek de gebruiker uit en klik op **„Wissen"** om deze gebruiker van de lijst te wissen

Gebruikersbeheer

Administrator: onbeperkte volledige toegang tot de videoserver.
Operator: geen toegang tot de configuratiepagina. Kan bijkomend URL-commando's uitvoeren (bijv. PTZ).
Gebruiker: de toegang is tot de hoofdpagina (live-view) beperkt.

Digitale uitgang: gebruikersgroep kan alarmingang en uitgang sturen
PTZ-besturing: gebruikersgroep heeft toegang tot de PTZ-besturing
Anonieme gebruikers toestaan: er vindt geen opvraag van gebruikersnaam en paswoord plaats bij het weergeven van de hoofdpagina.

6.3 HTTPS

Het HTTPS-protocol wordt voor de codering en de verificatie van de communicatie tussen webserver (videoserver) en browser (client pc) in het world wide web gebruikt. Alle gegevens die tussen videoserver en client-pc overgedragen worden, zijn met SSL gecodeerd. Voorwaarde voor HTTPS is naast de SSL-codering (compatibel met alle gangbare browsers) een certificaat dat de authenticiteit van de bron bevestigt.

HTTPS inschakelen

*Om HTTPS te kunnen gebruiken moet u eerst een certificaat aanmaken en installeren.

HTTPS beveiligde verbinding inschakelen:

Opslaan

Certificaat methode aanmaken en installeren

Creëer automatisch een zelf-ondertekend certificaat

Creëer handmatig een zelf-ondertekend certificaat:

Aanvraag voor een certificaat aanmaken en installeren:

Certificaatinformatie

Status: Niet geïnstalleerdV

Eigenschap Verwijderen

„ Veilige HTTPS-verbinding activeren" Naar keuze kan een ongecodeerde (HTTP) + gecodeerde (HTTPS) toegang of uitsluitend een gecodeerde (HTTPS) toegang toegestaan worden.

Bij een actieve veilige HTTPS-verbinding kan via de volgende regel toegang tot de videoserver verkregen worden:
https:\\„IP-Adresse"
Als u via de HTTPS-verbinding wilt streamen, gebruikt u de volgende link:
https:\\„IP-Adresse":„HTTPS-Port"\Live.sdp

Certificaten opstellen en instaleren

„Zelf ondertekend certificaat automatisch opstellen” Het in de videoserver voorgedefinieerde certificaat wordt gebruikt. Hierbij kunnen geen instellingen door de gebruiker uitgevoerd worden.

„Zelf ondertekend certificaat opstellen” Er wordt een nieuw certificaat opgesteld. Er moeten specifieke gegevens ingevoerd worden.

„Certificaataanvraag opstellen en installeren” Met deze optie kan een certificaataanvraag gegenereerd worden die bij een certificeringsinstantie ingediend kan worden. Er kan ook een door een erkende certificeringsinstantie (bijv.: VeriSign) uitgereikt certificaat op de videoserver geïnstalleerd worden.

Opmerking: Gebruikt u een „zelf ondertekend certificaat”, dan zult u evt. een waarschuwing van uw browser krijgen. Zelf ondertekende certificaten worden altijd door de webbrowser als onveilig beschouwd, omdat noch een stamcertificaat noch een echtheidsbewijs van een certificeringsinstantie voorhanden is.

6.4 SNMP

Het Simple Network Management Protocol is een netwerkprotocol om netwerktoestellen (bijv. router, server, switches, printer, computer enz.) vanuit een centraal station te kunnen bewaken en sturen. Het protocol regelt hierbij de communicatie tussen de bewaakte toestellen en het bewakingsstation. Activeer deze functie als u een SNMP-managementserver in uw netwerk inzet. U kunt ook naar softwareoplossingen teruggrijpen die op uw pc-systeem geïnstalleerd kunnen worden.

„Activeren van SNMPv1, SNMPv2c” Afhankelijk van de instellingen van uw SNMP-server kunt u hier naamvelden van de schrijf/leesgroepen vastleggen.

SNMP Configuratie

☑ Inschakelen SNMPv1, SNMPv2c

SNMPv1, SNMPv2c Instellingen

Lezen/schrijven groep: Private

Alleen lezen groep: Public

☐ Inschakelen SNMPv3

Opslaan

„Activeren van SNMPv3” Ondersteunt uw SNMP-server het SNMP-protocol in de versie 3, dan kunt u de statusopvragen gecodeerd uitvoeren. Hiervoor moet voor de vraag van de schrijf/leesgroepen een coderingsalgoritme en paswoord in de videoserver en SNMP-server opgeslagen worden.

6.5 Netwerk

6.5.1 Netwerkinstellingen

Alle wijzigingen die op deze pagina uitgevoerd worden, leiden tot het herstarten van het systeem om deze wijzigingen actief te laten worden. Zorg ervoor dat de velden telkens juist ingevuld zijn voor u op „Opslaan" klikt.

„LAN" De voorinstelling is LAN. Gebruik deze instelling als de videoserver met een LAN verbonden is. Hiervoor zijn bijkomende instellingen, zoals IP-adres of subnetmasker nodig.

„IP-adres automatisch verkrijgen" Bij elke herstart van de videoserver wordt aan dit adres een IP-adres via een DHCP-server toegewezen.

„Vast IP-adres gebruiken" De netwerkgegevens, zoals bijv. het IP-adres, worden hier vast gegeven.

„IP-adres" Dit adres is nodig voor de netwerkidentificatie.

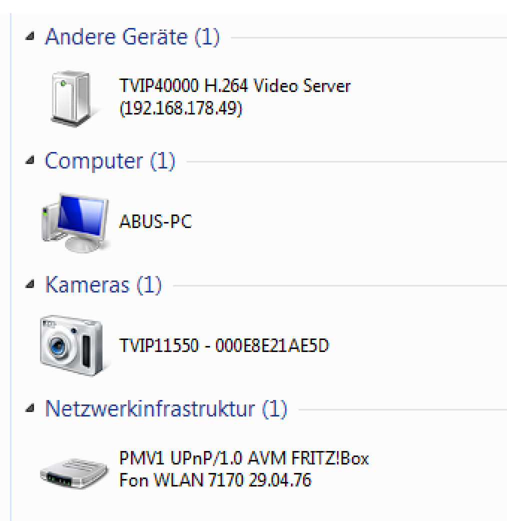
„Subnetmasker" Dient om te bepalen of het doel zich in hetzelfde subnet bevindt. De standaardwaarde luidt „255.255.255.0".

„Standaardrouter" Dit is de gateway voor het doorgeven van beelden aan een ander deelnet. Een ongeldige routerinstelling zal de overdracht aan deze doelen in verschillende deelnetten verhinderen. Bestaat een crosslinkkabelverbinding, gelieve dan hier absoluut een IP in hetzelfde subnetbereik van de videoserver in te voeren (bijv. 192.168.0.1).

„Primaire DNS" Server van de primaire domeinbenaming waarmee de hostnamen in IP-adressen omgezet worden.

„Secundaire DNS" Server van de secundaire domeinbenaming voor het maken van een reservekopie van de primaire DNS.

„UPnP gebruiken" De Universal Plug and Play wordt hiermee geactiveerd. Als uw besturingssysteem UPnP ondersteunt, kan de videoserver direct via het UPnP-beheer aangesproken worden (Windows: netwerkomgeving)



Zorg ervoor dat de optie „UPnP gebruiken" altijd geactiveerd is. UPnP wordt ook voor het vinden van de videoserver van eytron VMS gebruikt.

„UPnP poortverwijzing AAN” De Universal Plug and Play-poortverwijzing voor netwerkdiensten wordt hiermee geactiveerd. Ondesteunt uw router UPnP, dan wordt met deze optie automatisch de poortverwijzing voor videostreams aan routerzijde voor de videoserver geactiveerd.

„PPPoE” Gebruik deze instelling als de videoserver direct met een DSL-modem verbonden is. Gebruikersnaam en paswoord krijgt u van uw ISP (Internet Service Provider).

„IPv6” Gebruikt deze functie om met IP-adressen van de generatie v6 te werken.

☑ Inschakelen IPv6

IPv6 informatie

☑ IP-adres handmatig instellen

Optioneel IP-adres / Prefix lengte / 64

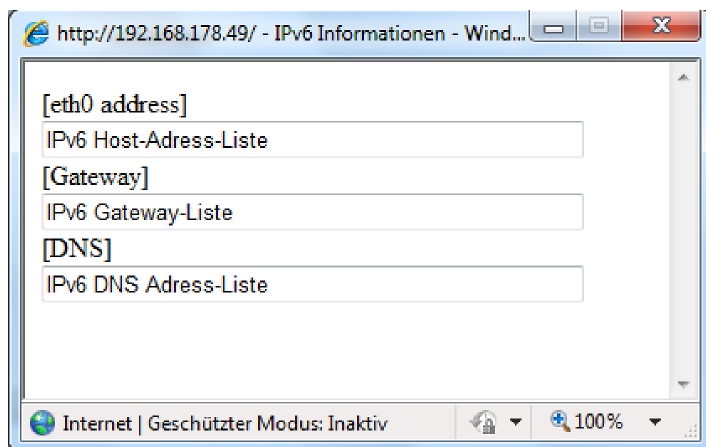
Optionele stadaard router

Optionele primaire DNS

Houd er rekening mee dat uw netwerk en de hardware IPv6 moeten ondersteunen.

Als IPv6 geactiveerd is, wacht de videoserver altijd tot hij van de router een IPv6 adres met DHCP toegewezen krijgt.
Als er geen DHCP-server voorhanden is, stelt u het IP-adres handmatig in.
Hiervoor „IP-adres handmatig instellen” activeren en IP-adres, standaard router en DNS-adres invoeren.

„IPv6 informatie” Alle IPv6 informatie wordt in een afzonderlijk venster weergegeven.



Als de IPv6 instellingen correct zijn, kunt u alle instellingen in het onderste venster aflezen.

[eth0 address]

2001:0c08:2500:0002:0202:d1ff:fe04:65f4/64@Global

fe80:0000:0000:0000:0202:d1ff:fe04:65f4/64@Link

[Gateway]

fe80::211:d8ff:fea2:1a2b

[DNS]

2010:05c0:978d::

6.5.2 IEEE 802.1x

Activeer deze functie als uw netwerkomgeving de standaard IEEE 802.1x, een op een poort gebaseerde toegangscontrole in het netwerk, gebruikt.
IEEE 802.1x verbetert de veiligheid van lokale netwerken.
Een verbinding wordt alleen toegestaan als alle certificaten tussen server en „klant" geverifieerd werden. Dit gebeurt door een verificateur in de vorm van een switch/access point dat aanvragen naar de RADIUS verificatieserver stuurt.
Anders wordt geen verbinding tot stand gebracht en de toegang tot de poort wordt geweigerd.

Houd er rekening mee dat uw netwerkcomponenten alsook de RADIUS-server de standaard IEEE 802.1x moeten ondersteunen.

6.5.3 HTTP

„**HTTP-poort**" Dit kan een andere poort dan de opgegeven poort 80 zijn (80 of 1025 – 65535). Na het wijzigen van de poort moet de gebruiker over de wijziging geïnformeerd worden om een succesvolle verbinding te garanderen. Als de administrator bijvoorbeeld de HTTP-poort van de videoserver, waarvan het IP-adres 192.168.0.99 is, van 80 naar 8080 wijzigt, dan moet de gebruiker in de plaats van „http://192.168.0.99" „http://192.168.0.99:8080" in de webbrowser invoeren.

"**Secundaire HTTP-poort**" Bijkomende HTTP-poort voor de videoservertoegang

Voor de directe toegang tot individuele videostreams via het web zijn de volgende toegangsnamen instelbaar. De toegang gebeurt via gecomprimeerde JPEG-beelden en maakt voor webbrowsers (Firefox, Netscape), die geen ActiveX-Plugin kunnen verwerken, de directe toegang tot de videostream mogelijk:

„Toegangsnaam voor stream 1" Toegangsnaam voor de MJPEG stream 1
„Toegangsnaam voor stream 2" Toegangsnaam voor de MJPEG stream 2
„Toegangsnaam voor stream 3" Toegangsnaam voor de MJPEG stream 3
„Toegangsnaam voor stream 4" Toegangsnaam voor de MJPEG stream 4

Opmerking: Internet Explorer ondersteunt geen weergave van MJPEG-beelden zonder Active X

6.5.4 FTP

„**FTP-poort**" Dit is de interne FTP-serverpoort. Dit kan een andere poort dan de opgegeven poort 21 zijn (21 of 1025 – 65535). Via FTP kunnen de op de videoserver opgeslagen videogegevens direct opgeroepen worden. Gebruik hiervoor een zelfstandig FTP-programma.

Het adresformaat voor het invoeren van de verbindingsgegevens is als volgt opgebouwd:
Server: IP-adres van de videoserver
Gebruikersnaam: administratorgebruiker
Paswoord: paswoord van de administrator
Poort: FT¨P-poort van de videoserver

Voorbeeld (met FTP-programma)
Server: 192.168.0.99
Gebruikersnaam: root
Paswoord: admin
Poort: 1026

Server: /mnt/auto/CF/NCMF

/
mnt
auto
CF
NCMF
ncmf
CF

Dateiname /	Dateigröße	Dateityp	Zuletzt geändert	Berechtigu...	Besitzer/Gr...
000_1283513262.jpg	77.915	JPEG-Bild	03.09.2010 11:2...	-rwxr-xr-x	root root
000_1283513305.jpg	77.966	JPEG-Bild	03.09.2010 11:2...	-rwxr-xr-x	root root
000_1283513366.jpg	77.821	JPEG-Bild	03.09.2010 11:2...	-rwxr-xr-x	root root
000M.jpg	77.098	JPEG-Bild	03.09.2010 11:2...	-rwxr-xr-x	root root
001.jpg	77.218	JPEG-Bild	03.09.2010 11:2...	-rwxr-xr-x	root root
001M.jpg	77.259	JPEG-Bild	03.09.2010 11:2...	-rwxr-xr-x	root root
001M_1283513256.jpg	77.638	JPEG-Bild	03.09.2010 11:2...	-rwxr-xr-x	root root
001M_1283513303.jpg	78.269	JPEG-Bild	03.09.2010 11:2...	-rwxr-xr-x	root root
001M_1283513364.jpg	77.926	JPEG-Bild	03.09.2010 11:2...	-rwxr-xr-x	root root
002.jpg	77.267	JPEG-Bild	03.09.2010 11:2...	-rwxr-xr-x	root root
002_1283513268.jpg	78.236	JPEG-Bild	03.09.2010 11:2...	-rwxr-xr-x	root root
002_1283513310.jpg	78.411	JPEG-Bild	03.09.2010 11:2...	-rwxr-xr-x	root root
002_1283513368.jpg	77.496	JPEG-Bild	03.09.2010 11:2...	-rwxr-xr-x	root root
20100903_112614.mp4	542.681	MPEG-4 M...	03.09.2010 11:2...	-rwxr-xr-x	root root
20100903_112711.mp4	546.532	MPEG-4 M...	03.09.2010 11:2...	-rwxr-xr-x	root root
20100903_112819.mp4	547.002	MPEG-4 M...	03.09.2010 11:2...	-rwxr-xr-x	root root
normal-1283513308_2073467...	35.217.960	3GPP Movie	03.09.2010 11:2...	-rwxr-xr-x	root root
normal-1283513368_1099627...	2.565.197	3GPP Movie	03.09.2010 11:2...	-rwxr-xr-x	root root

19 Dateien und 2 Verzeichnisse. Gesamtgröße: 40.507.467 Bytes

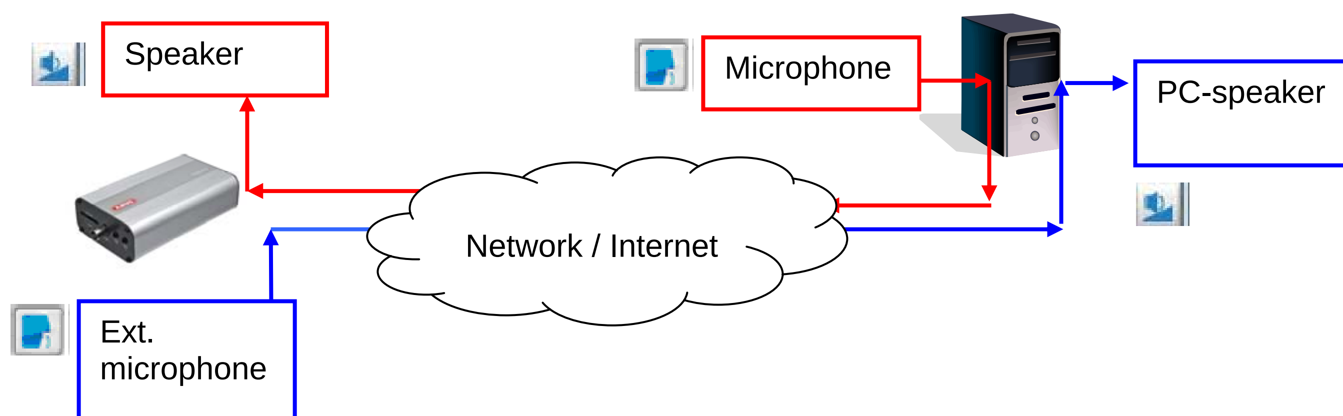
6.5.5 HTTPS

„**HTTPS-poort**" Dit is de poortinstelling voor de interne HTTPS-poort. Dit kan een andere poort dan de opgegeven poort 443 zijn (443 of 1025 – 65535). Andere instellingsmogelijkheden voor HTTPS vindt u op 5.5.3

6.5.6 Tweewegaudio

„Tweewegaudio" Dit is de poort voor de tweewegaudiofunctie. Dit kan een andere poort dan de opgegeven poort 5060 zijn (5060 of 1025 – 65535).

Om de tweewegaudiofunctie te kunnen gebruiken, moet u onder **„Video en audio"** voor de gekozen videostream MPEG-4/H.264 activeren. MJPEG ondersteunt uitsluitend de overdracht van videogegevens en is daarom voor deze functie niet geschikt.



Livestreamfuncties:

Start de overdracht van de audiogegevens.

Regelt de gevoeligheid van de audio-ingang van de videoserver.

Schakel de microfoon/audio-ingang uit.

Klik opnieuw op de knop om de audio-overdracht te stoppen.

6.5.7 RTSP overdracht

„**RTSP-verificatie**" De verificatie kan disable (standaard) of Basic (eenvoudig) of uitgebreide modus (digest) zijn.

Is de RTSP-verficatie geactiveerd, dan moet bij de RTSP-verbindingsopbouw een gebruikersnaam en een paswoord van een geldige gebruiker ingevoerd worden (bijv. administrator).
OPMERKING: De RTSP verificatie moet door de videospeler ondersteund worden (bijv. Realplayer 10.5).

„Toegangsnaam voor stream 1" Dit is de toegangsnaam 1 om een verbinding van een client tot stand te brengen. Het Codectype moet MPEG4 zijn! Gebruik
rtsp://<IP-adres>:RTSP-poort /<Toegangsnaam 1> om een verbinding tot stand te brengen.

„Toegangsnaam voor stream 2" Dit is de toegangsnaam 2 om een verbinding van een client tot stand te brengen. Het Codectype moet MPEG4 zijn! Gebruik
rtsp://<IP-adres>:RTSP-poort /<Toegangsnaam 2> om een verbinding tot stand te brengen.

„Toegangsnaam voor stream 3" Dit is de toegangsnaam 3 om een verbinding van een client tot stand te brengen. Het Codectype moet MPEG4 zijn! Gebruik
rtsp://<IP-adres>:RTSP-poort /<Toegangsnaam 3> om een verbinding tot stand te brengen.

„Toegangsnaam voor stream 4" Dit is de toegangsnaam 4 om een verbinding van een client tot stand te brengen. Het Codectype moet MPEG4 zijn! Gebruik
rtsp://<IP-adres>:RTSP-poort /<Toegangsnaam 4> om een verbinding tot stand te brengen.

RTSP toegang met VLC:
rtsp://192.168.0.99:10052/live.sdp

„RTSP-poort" Deze poort kan van de vooringestelde poort 554 afwijken (554; of 1025 tot 65535). Neem bij wijziging het invoerformaat analoog met de HTTP-poort in acht.

„RTP-poort voor videov**"** Deze poort kan van de vooringestelde poort 5558 afwijken. Het poortnummer moet even zijn.

„RTCP-poort voor video" Deze poort moet de „RTP-poort voor video" plus 1 zijn.

„RTP-poort voor audio" Deze poort kan van de vooringestelde poort 5556 afwijken. Het poortnummer moet even zijn.

„RTCP-poort voor audio" Deze poort moet de „RTP-poort voor audio" plus 1 zijn.

6.5.8 Multicast-overdracht

Multicast staat voor een berichtoverdracht van een punt naar een groep (ook multipuntverbinding genoemd). Het voordeel van multicast bestaat erin dat tegelijk berichten aan meerdere deelnemers of aan een gesloten deelnemergroep overgedragen kunnen worden zonder dat de bandbreedte zich bij het zenden met het aantal ontvangers vermenigvuldigd. De zender heeft bij de multicasting slechts dezelfde bandbreedte als een individuele ontvanger nodig. Er vindt een vermenigvuldiging van de pakketten aan elke netwerkverdeler (switch router) plaats.

Multicast maakt het IP-netwerken mogelijk om efficiënt gegevens naar veel ontvangers tegelijk te sturen. Dat gebeurt met een speciaal multicastadres. In IPv4 is hiervoor het adresbereik 224.0.0.0 tot 239.255.255.255 gereserveerd.

De volgende multicastinstellingen kunnen voor stream 1 – 4 in de videoserver geconfigureerd worden.

„Altijd multicast" activeren om multicast te gebruiken.

„Multicast groepsadres" Specificeert een groep van IP-hosts die bij deze groep behoren

„Multicast videpoort" Deze poort kan van de vooringestelde poort 5560 afwijken. Het poortnummer moet even zijn.

„Multicast RTCP videopoort" Deze poort moet de „Multicast videopoort" plus 1 zijn.

„Multicast audiopoort" Deze poort kan van de vooringestelde poort 5562 afwijken. Het poortnummer moet even zijn.

„Multicast RTCP audiopoort" Deze poort moet de „Multicast audiopoort" plus 1 zijn.

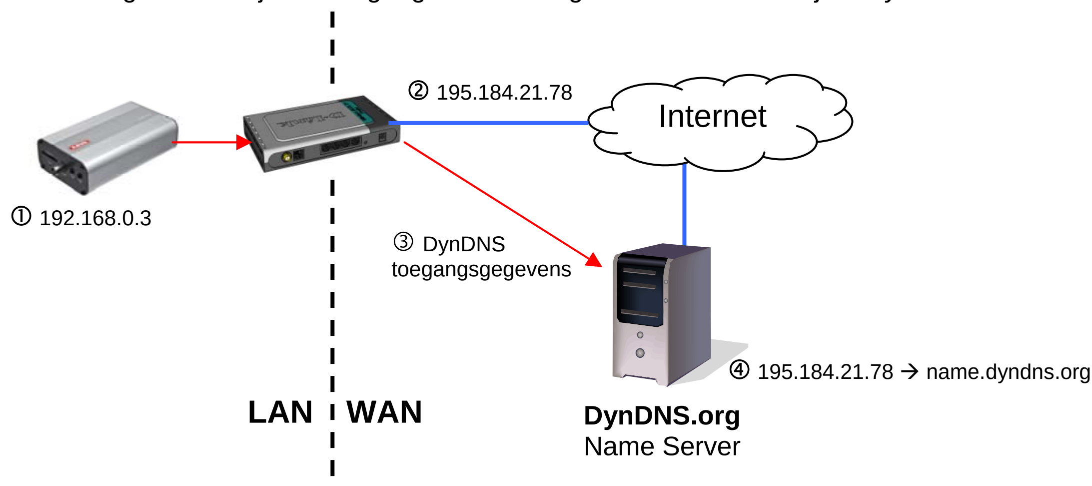
„Multicast TTL" Time to Live

Als u een poortdoorschakeling in een router instelt, dan moeten altijd alle poorten doorgeschakeld worden (RTSP + HTTP). Dit is voor een succesvolle communicatie nodig.

7. DDNS

DynDNS of DDNS (dynamische Domain-Name-System-entry) is een systeem dat in real time domain-name-entry's kan actualiseren. De videoserver beschikt over een geïntegreerde DynDNS-client die zelfstandig de actualisering van het IP-adres bij een DynDNS-aanbieder kan uitvoeren. Als de videoserver zich achter een router bevindt, raden we aan om de DynDNS-functie van de router te gebruiken.

De afbeelding verduidelijkt de toegang/actualisering van het IP-adres bij de DynDNS-dienst.



„DDNS activeren" Met deze optie wordt de DDNS-functie geactiveerd.

„Dienstaanbieder" De aanbiederlijst bevat hosts die de DDNS-diensten aanbieden. Breng een verbinding met de website van de dienstverlener tot stand om er zeker van te zijn dat de dienst beschikbaar is.

„Hostnaam" Voor de toepassing van de DDNS-dienst moet dit veld ingevuld worden. Voer de hostnaam in die bij de DDNS-server geregistreerd is.

„Gebruikersnaam/e-mail" De gebruikersnaam en de e-mail moeten in het veld ingevoerd worden om een verbinding met de DDNS-server tot stand te brengen of om de gebruikers over het nieuwe IP-adres te informeren. Aanwijzing: wordt in dit veld de „gebruikersnaam" ingevoerd, dan moet in het volgende veld het „paswoord" ingevoerd worden.

„Paswoord" Voor het gebruik van de DDNS-dienst voert u hier uw paswoord in.

DDNS: Dynamic domain name service

DDNS inschakelen:

Aanbieder: Dyndns.org(Dynamic)

Hostnaam:

Gebruikersnaam:

Wachtwoord:

Opslaan

7.1 DDNS account installeren

Nieuwe account bij DynDNS.org installeren

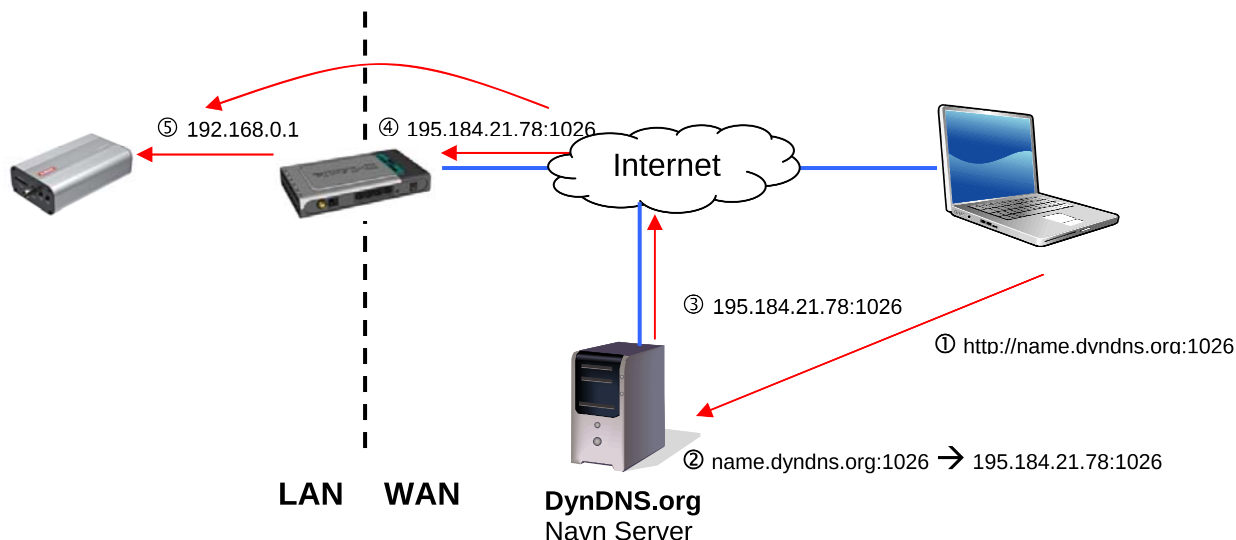
Accountinformatie opslaan

Noteer uw gebruikersgegevens en voer deze in de configuratie van de videoserver in.

7.2 DDNS-toegang via router

Als uw netwerkvideoserver zich achter een router bevindt, dan moet de toegang via DynDNS in de router geconfigureerd worden. Hiervoor vindt u op de ABUS Security-Center homepage www.abus-sc.com een beschrijving voor de DynDNS-routerconfiguratie voor gangbare routermodellen.

De volgende afbeelding verduidelijkt de toegang tot een videoserver achter een router via DynDNS.org.



Voor de DynDNS-toegang via een router moet een poortdoorschakeling van alle relevante poorten (minstens RTSP + HTTP) in de router ingesteld worden.

8. Toegangslijst

Hier stuurt u de toegang tot de videoserver aan de hand van IP-adreslijsten.

„Max. aantal gelijktijdige verbindingen beperkt tot” Aantal tegelijkertijd mogelijke verbindingen met de videoserver. Afhankelijk van de ter beschikking staande bandbreedte van de videoserver kan het nuttig zijn om de toegang te beperken.
„Toegangslijst activeren” Activeert de onder „Filter” gedefinieerde IP-adresfilter.

U hebt twee mogelijkheden om de IP-adresfiltering te definiëren.

- Filtertype „toestaan”: alleen IP-adressen in de gedefinieerde adresruimte hebben toegang
- Filtertype „weigeren”: IP-adressen in de gedefinieerde adresruimte hebben geen toegang

Klik op „Toevoegen” om de adresbereiken te configureren. De volgende instellingsmogelijkheden zijn gegeven:

Algemene instellingen

Maximum aantal gelijktijdige streamverbindingen beperkt tot: 10 [Informatie weergeven]

☐ Filtering toegangslijst inschakelen

[Opslaan]

Filter type

○ Toestaan ◉ Weigeren

[Opslaan]

Filters

IPv4 toegangslijst

[Toevoegen] [Wissen]

IP-adres beheerder

☐ Dit IP-adres altijd toegang geven tot dit apparaat

[Opslaan]

Regel: individueel, bereik, netwerk:

- Individueel: een specifiek IP-adres wordt toegevoegd
- Bereik: er kunnen IP-adresbereiken van – tot vastgelegd worden
- Netwerk : er kunnen IP-adressen met specifiek subnetmasker vastgelegd worden

adres filteren

Regel: Enkel

IP adres

Enkel
Netwerk
Bereik

[OK] [Annuleren]

Voorbeeld:
Het IP-adresbereik van 192.168.0.1 tot 192.255.255.255 moet toegestaan worden.
Volgende IP-adressen moeten geblokkeerd worden 192.168.1.0 tot 192.168.255.255

Resultaat:
er mogen alleen toegangspogingen van IP's op het volgende bereik uitgevoerd worden:
192.168.0.1 – 192.168.0.255

Er wordt altijd een gemiddelde hoeveelheid tussen toegestane toegangspogingen en geblokkeerde IP’s gevormd.

9. Audio en video

Video-instellingen

Videotitel:

Kleur: Kleur

Modulatie: Automatisch

Cachestream kiezen: Stream 4

Video-oriëntatie: Flip Mirror

Titel en tijd in video en snapshot weergeven.

Afbeeldingsinstellingen Privacymasker

Instellingen videokwaliteit voor stream 1:

Instellingen videokwaliteit voor stream 2:

Instellingen videokwaliteit voor stream 3:

Instellingen videokwaliteit voor stream 4:

Audio-instellingen

Dempen

Externe microfoonaansluiting: 0 dB

Audio type:

AAC:

AAC bitrate: 16 Kbps

GSM-AMR:

G.711:

Modus: pcmu

Opslaan

„Videotitel” De tekst verschijnt in de zwarte balk boven het videovenster met een tijdstempel. Deze tijdstempel (datum en tijd) wordt door de geïntegreerde realtimeklok van de videoserver geleverd.

„Kleur” Kies uit weergave in kleur en zwar/wit.

„Modulatie” Kies tussen de videostandaard NTSC en PAL of een automatische herkenning van het videosignaal door de videoserver.

„Videobuffer” De geselecteerde videostream wordt voor de opname van voor- en na-alarmvideogegevens (zie hoofdstuk „Toepassing”) gebruikt.

„Kantelen” Voor het horizontaal roteren van de video. Kies deze opties als de camera omgekeerd geïnstalleerd werd.

„Spiegelen” Voor het verticaal roteren van de video.

Gebruik de optie kantelen + spiegelen als de camera aan het plafond geïnstalleerd is.

„Videotitel en tijdstempel weergeven” Met deze optie kunnen titel en tijdstempel direct in het videobeeld en momentopnames weergegeven worden. De gegevens onder punt „Videotitel” worden hier gebruikt.

9.1 Beeldinstellingen

„Helderheid, contrast, verzadiging, scherpte”
Pas de waarde volgens de lichtomstandigheden aan.

Beeldaanpassing
Helderheid: +0
Verzadiging: +0
Contrast: +0
Scherpte: +0
Voorbeeldweergave Herstellen Opslaan
Sluiten

Als de lichtverhoudingen van de camera veranderen, kunnen de beeldinstellingen voor slechte lichtverhoudingen, bij goede lichtverhoudingen een negatieve invloed op de beeldkwaliteit hebben .

Om de gewijzigde instellingen van de beelden te bekijken, klikt u op „Voorbeeld”. Om de beeldparameters over te nemen, klikt u op „Opslaan”. Wilt u de wijzigingen niet overnemen, klik dan op „Herstellen”.

9.2 Maskeren van privézones

Met deze functie kunnen bereiken in het videobeeld uitgeschakeld worden. Er kunnen maximaal 5 willekeurig grote bereiken gemarkeerd worden.

Activeer eerst deze functie door het plaatsen van het vinkje bij **„Maskeren privé-zone activeren”**.

Met de knop **„Nieuw”** wordt een nieuw venster aangemaakt, waarvan de grootte erna aangepast kan worden. Druk op **„Opslaan”** om de instellingen over te nemen.

Privémaskering inschakelen
(UDP-V) 2010/09/09 13:38:42
Test
Vensternaam
Test
X32 Breedte168
Y32 Hoogte152
Nieuw Opslaan

Deze functie mag niet geactiveerd worden als de PTZ/ePTZ-functie van de camera gebruikt wordt. Deze functie kan alleen geconfigureerd worden als als browser MS Internet Explorer gebruikt wordt (ActiveX Modus).

9.3 Basisinstelling:

Video-opties
De videoserver stelt voor het flexibele gebruik vier videostreams in verschillende resoluties ter beschikking.

- Instellingen videokwaliteit voor stream 1:
- Instellingen videokwaliteit voor stream 2:
- Instellingen videokwaliteit voor stream 3:
- Instellingen videokwaliteit voor stream 4:

Instellingen van de streams 1, 2, 3 en 4
Via het betreffende menu configureert u stream 1 – 4

De resolutie bij stream 4 is op QCIF vastgelegd. Om op mobiele toestellen te streamen, gebruikt u stream 4.

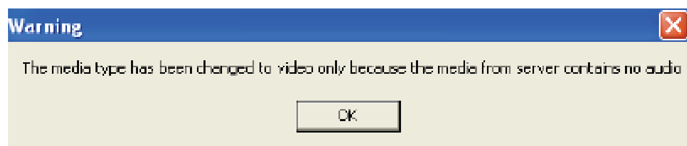
„Beeldcompressie" Kies tussen H.264/MPEG-4/MJPEG.
„Beeldformaat" Stel hier de gewenste resolutie in.
„Max. Beeldfrequentie" Stel hier de maximale beeldherhalingssnelheid in.
„Sleutelbeeldinterval" Legt vast hoe vaak een I-frame gecreëerd wordt. Hoe korter het interval, hoe beter de beeldkwaliteit, in elk geval ten koste van een hogere netwerkbelasting.
„Videokwaliteit vaste beeldsnelheid" Legt de beeldsnelheid constant op een waarde vast.
De beeldkwaliteit daalt bij toename van de beeldcomplexiteit (bijv.: beweging).
„Vaste beeldkwaliteit" Legt de beeldkwaliteit op een constante waarde vast. De bitsnelheid stijgt bij toename van de beeldcomplexiteit (bijv.: beweging).

Compressie → / Opnameduur ↓	**H.264**	**MPEG-4**	**MJPEG**
1 minuut videosequentie in D1 resolutie met kwaliteit „goed"	Ca. **12** MB	Ca. **14** MB	Ca. **60** MB
Geheugencapaciteit **32 GB** SD-kaart	Ca.**43** uur	Ca.**36** uur	Ca.**9** uur

Op het einde van de handleiding vindt u een gedetailleerde tabel met elke kwaliteitsinstelling gecombineerd met elke resolutie.

9.4 Audio-instellingen

„Mute” Alle audiofuncties in de videoserver worden gedeactiveerd. Er verschijnt een aanwijzing bij de toegang tot de videoserver.



„Externe microfoon/audio-input versterking” Pas de waarde van +21db tot -33db aan

„Audiotype” Kies hier het audiotype en de gewenste bitsnelheid. Een hogere waarde vereist meer bandbreedte:

- **„AAC”** (Advanced Audio Coding) Speciale codec voor audiogegevenscompressie onder MPEG-4/H.264.
- **„GSM-AMR”** (Global System for Mobile Communications - Adaptive Multi Rate) spraakcodec in het mobiele gsm-netwerk.
- **„G.711”** pmca/pmcu (Puls Code Modulation)

10. Bewegingsherkenning

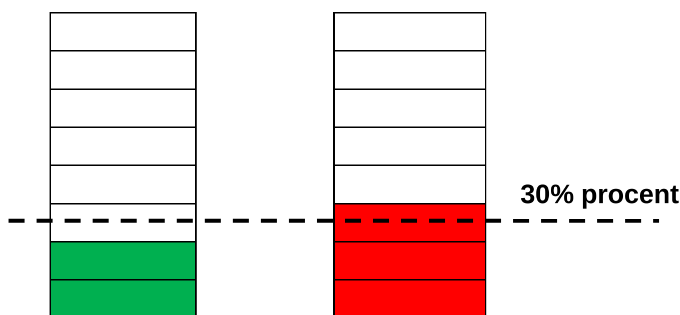
Er kunnen drie bewegingszones in de videoserver geactiveerd worden. Kies **„Bewegingsmelder activeren”** om de configuratie uit te voeren.

De functie bewegingsherkenning is pas na het vastleggen van een actie onder het menupunt „Toepassing” actief.

„Vensternaam” De tekst verschijnt van boven in het venster.
„Gevoeligheid” Gevoeligheid bij veranderingen in het beeldverloop (bijv.: gevoeligheid hoog: resolutie bij geringe beeldwijziging.
„Procent” Geeft aan hoeveel procent van het beeld moet veranderen opdat de bewegingssensor geactiveerd wordt.

„Nieuw” Klik op deze knop om een nieuw venster toe te voegen. Voor het opnieuw instellen van de grootte van het venster of voor het verplaatsen van de titelbalk klikt u met de linker muisknop op het kader van het venster, u houdt deze ingedrukt en u trekt het kader met de cursor op de gewenste grootte. Door het aanklikken van de „x” in de hoek bovenaan rechts van het venster wordt het venster gewist.
„Opslaan” Klik op deze knop om de betreffende instellingen van het venster op te slaan. Afhankelijk van de beeldvariatie stijgt of daalt een grafische balk.

Een groene balk betekent dat de beeldvariatie zich onder het bewakingsniveau bevindt, terwijl een rode balk erop wijst dat de beeldvariatie zich boven het bewakingsniveau bevindt. Is de balk rood, dan verschijnt het herkende venster eveneens met een rode omranding. Bij het teruggaan naar de homepage wordt het bewaakte venster niet weergegeven. Het rode kader wordt echter weergegeven zodra een beweging herkend wordt.



Groen bereik: beweging werd herkend, maar leidt niet tot een activering van het alarm
Roode bereik: beeldvariatie (beweging) overstijgt de grenswaarde van 30% en leidt tot een alarm.

Werkwijze van de bewegingsherkenning:

U hebt twee parameters om de beweringsherkenning in te stellen: **gevoeligheid** en **procent**. De afbeelding verklaart hoe deze beide parameters de bewegingsherkenning beïnvloeden.

Uitgaande van afbeelding A vindt een beweging naar beeld B plaats. De resulterende pixelwijzigingen (afhankelijk van de gevoeligheidsinstelling) worden in afbeelding C weergegeven (grijs). De instelling **„Gevoeligheid"** heeft betrekking op het vermogen van het sensorsysteem om bewegingen in het beeld te herkennen. Hoe hoger deze waarde ingesteld is, hoe meer pixelwijzigingen op het beeld herkend worden. Bij een bewegingsherkenning worden de pixelwijzigingen (afhankelijk van de gevoeligheid) serverintern als alarmpixels opgeslagen (roze velden in afbeelding D). De drempelwaarde **„Procent"** beschrijft hierbij het aandeel van de „alarmpixels" t.o.v. het aantal pixels in het geselecteerde bereik. Wordt het vastgelegde aandeel alarmpixels (procent) bereikt/overschreden, wordt een alarm geactiveerd. Voor een betrouwbare bewegingsherkenning is het aan te bevelen om een hoge gevoeligheid en een lage procentwaarde in te stellen.

11. Camera sabotageherkenning

De videoserver ondersteunt een sabotageherkenning. Is de herkenning geactiveerd, kan een resulterend alarm als gebeurtenis voor een bericht gebruikt worden (zie toepassing)

„Videoserver sabotagebeveiliging activeren” Het sensorsysteem wordt geactiveerd.

„Activeringsgedrag” De periode definieert hoe lang een sabotagegebeurtenis voorhanden moet zijn tot een alarm geactiveerd wordt.

De volgende sabotagegebeurtenissen worden gecontroleerd:

- Verdraaien camera
- Afdekken camera
- Focussering camera

Deze sabotageherkenning kunt u als activering in de camerafunctie „Toepassing/gebeurtenissetup” gebruiken.

12. Camerabesturing

De videoserver biedt de mogelijkheid om een analoge PTZ-camera te sturen.

RS485-instellingen

„Gedeactiveerd” RS485-besturing is uitgeschakeld

„PTZ-camera” Voer hier de betreffende parameters van de PTZ-camera in. De volgende protocollen worden ondersteund: Pelco-D, Pelco-P, Samsung scc643, DynaDome/SmartDOME, Lilin PIH-7x00.
Als u PTZ-camera geen van deze protocollen ondersteunt, kies dan „Custom camera”

„Transparante HTTP-tunnel” Ondersteunt uw PTZ-toestel RS485-commando’s via een netwerkinterface, dan kunt u deze optie kiezen. De nodige parameters kunt u in de gebruiksaanwijzing van uw PTZ-toestel terugvinden.

RS485 instellingen

Uitschakelen

PTZ camera

Transparante HTTP tunnel

Camera ID: 1

PTZ stuurprogramma: Pelco D protocol

Poortinstellingen:

Baudrate: 2400

Gegevensbits: 8

Stopbits: 1

Pariteitsbit: geen

Presetpositie | Aangepaste opdracht

Opslaan

De genoemde PTZ-commando's vindt u in de gebruiksaanwijzing van uw PTZ-toestel.

„Kamera ID” Legt de camera ID vast.
„PTZ driver” Legt het protocol van het aangesloten PTZ-toestel vast.
„Baudsnelheid” Stel de passende baudsnelheid in.

„Databits” Stel de passende databits in.
„Stopbits” Stel de passende stopbits in.
„Pariteit” Legt de pariteit vast.

Presetposities en toer instellen

Er kunnen in het totaal 20 presetposities in de videoserver opgeslagen worden. Ga hiervoor als volgt te werk:

1. Plaats het camerabeeld met de pijltoetsen op de gewenste instelling.
2. Geef aan de actuele positie een presetnaam en klik op toevoegen. De naam verschijnt in de presetlijst.
3. Herhaal de stappen 1-2 voor bijkomende presets
4. Markeer de presets die u voor een toer wilt gebruiken en bevestig deze met „Kiezen”.
5. Pas de verblijftijd van de betreffende preset indien nodig aan.
6. Sla de instellingen op.

Bewaking keuze:

Opslaan

Sluiten

Om de toer te starten, drukt u op „PATROL” in het livebeeld van de videoserver. Om deze te stoppen, drukt u op „STOP”

Gebruikersgedefinieerd commando

Het menupunt „Gebruikersgedefinieerd commando” maakt voor u de directe toegang tot verschillende functies van uw PTZ-toestel of de PTZ-camera mogelijk.
In de regel wordt de functie gebruikt om opgeslagen presetposities of voorgedefinieerde toeren op te roepen.

Aangepaste opdracht

Wanneer de "Knopnaam" leeg blijft, wordt de knop niet op de startpagina weergegeven.

	Knopnaam	Commando
Commando 1:	TOUR 1	FF0100900010B
Commando 2:		
Commando 3:		
Commando 4:		
Commando 5:		

Opslaan Sluiten

Met behulp van deze functie kunt u enkele commandoknoppen in het livebeeld van de videoserver voor de bediening/instelling van het aangesloten PTZ-toestel creëren.
De betreffende functie van de knop wordt door een hexadecimale code (afhankelijk van het betreffende PTZ-protocol) beschreven.
Alle ABUS speeddomecamera’s gebruiken de protocollen PELCO D/P.
Er kunnen maximaal 5 gebruikersgedefinieerde knippen gecreëerd worden.
Onder „Knopnaam” voert u de gewenste naam van de knop in (bijv.: Toer 1).

Als u als cameraprotocol „Custom camera” ingevoerd hebt, dan moet u onder „Gebruikersgedefinieerd commando” fundamentele functies, zoals „omhoog”, „omlaag”, „links”, „rechts” vastleggen. De hiervoor van toepassing zijnde codes vindt u in de handleiding van het PTZ-toestel.

Wordt er geen knopnaam aangegeven, dan verschijnt de knop niet in het livebeeld

Het Pelco D/P protocol werkt uitsluitend met hexadecimale getallen.

Voer onder „Commando” de HEX-code van de gewenste functie in.
(bijv.: FF 01 00 09 00 01 0B**)**

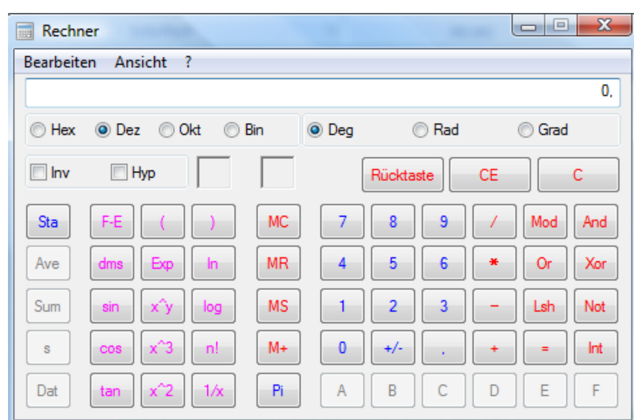
De code mag geen spaties en speciale tekens bevatten.
FF 01 00 09 00 01 0B → FF01000900010B

Voorwaarde hexadecimale getallen
In het volgende hoofdstuk wordt aan de hand van enkele voorbeelden het hexadecimale getallensysteem verklaard.

Decimal	Hex	Decimal	Hex	Decimal	Hex
1	1	11	B	30	1E
2	2	12	C	40	28
3	3	13	D	50	32
4	4	14	E	60	3C
5	5	15	F	70	46
6	6	16	10	80	50
7	7	17	11	90	5A
8	8	18	12	100	64
9	9	19	13	500	1F4
10	A	20	14	1000	3E8

Het hexadecimale getallensysteem is gebaseerd op getallen van 0-9 en letters van A-F. Bij de berekening van checksommen moet er rekening mee gehouden worden dat hexadecimaal opgeteld wordt.

Een belangrijke hulp voor de omrekening van decimaal naar hexadecimaal en optellen van hexadecimaal biedt hiervoor de in Microsoft Windows geïntegreerde rekenmachine, die hiervoor op „wetenschappelijk” ingesteld moet zijn.



Dome-stuurcommando's voor TV7600, TV6702, TV7604 (Pelco)

Commandosamenstelling

Woord 1	Woord 2	Woord 3	Woord 4	Woord 5	Woord 6	Woord 7
Synch Byte (altijd FF)	Address (ID van de analoge camera)	Command 1	Command 2	Data 1	Data 2	Check Sum Woord 2-6

Berekening checksom:

Woord 7 = woord 2 + woord 3 + woord 4 + woord 5 + woord 6

Woordverklaring:

„Woord1" Altijd als „FF" opgegeven
„Woord2" Bepaalt de ID van de analoge camera
„Woord3"- „Woord4" Legt de verschillende PTZ-functies vast („Sla preset op", „Start toer" enz.)
„Woord5"-„Woord6" Legt bijvoorbeeld de nummering van de presets en toeren vast.
Als u een preset wilt aanlopen, dan moet ook vastgelegd worden welk presetnummer aangelopen moet worden.
„Woord7" Is de som van woord 2 – woord 6 en is ook als checksom bekend

Voorbeeld: „Ga naar preset 1" heeft het bevel: FF 01 00 07 00 **01** 09

Woord 1 is altijd op FF vastgelegd
Woord 2 is altijd de ID van de speeddome
Woord 3 en woord 4 bepalen de functie: „Naar preset gaan"
Woord 5 en woord 6 bepaalt welke preset aangelopen moet worden.
Woord 7 checksom

Uitleg: In woord 6 staat het hexadecimale getal 01 voor preset 1.
Als men nu preset 15 zou willen aanlopen, dan zou men 0F in het woord 6 moeten schrijven.

Voorbeeld: „Ga naar preset 15" heeft het bevel: FF 01 00 07 00 **0F** 17
Deze werkwijze is analoog bij de keuze van toeren of andere telbare functiestructuren.

Voorbeeld: „Ga naar preset 15" heeft het bevel: FF 01 00 07 00 **0F** 17
Deze werkwijze is analoog bij de keuze van toeren of andere telbare functiestructuren.

Beveloverzicht:

Commando	Woord 3	Woord 4	Woord 5	Woord 6
Naar beneden	00	10	00	2A
Naar boven	00	08	00	3C
Links draaien	00	04	2E	00
Rechts draaien	00	02	06	00
Stoppen	00	00	00	00
Menu	00	11	00	00
Toer starten	00	00	09	01 to 08
Scan	00	0F	00	01
Zoom tele	00	20	00	01
Zoom wide	00	40	00	01
Focus near	01	00	00	01
Focus far	00	80	00	00
Iris close	04	00	00	00
Iris open	02	00	00	00
Preset opslaan	00	03	00	01 to C8
Wis preset	00	05	00	01 to C8
Ga naar preset	00	07	00	01 to C8
Set Auxiliary	00	09	00	01 to 08
Clear Auxiliary	00	0B	00	01 to 08
Remote Reset	00	0F	00	00
Set Zone Start	00	11	00	01 to 08
Set Zone End	00	13	00	01 to 08
Write Char. To Screen	00	15	X Position 00 to 28	ASCII Value
Clear Screen	00	17	00	00
Alarm Acknowledge	00	19	00	Alarm No.
Zone Scan aan	00	1B	00	00
Zone Scan uit	00	1D	00	00
Voorbeeldstart instellen	00	1F	00	00
Voorbeeldstop instellen	00	21	00	00
Patroon aansturen	00	23	00	00
Stel zoomspeed in	00	25	00	00 to 03
Stel Focus Speed in	00	27	00	00 to 03
Fabrieksinstelling van de camera	00	29	00	00
Autofocus auto/aan/uit	00	2B	00	00-02
Auto Iris auto/aan/uit	00	2D	00	00-02
AGC auto/aan/uit	00	2F	00	00-02
BLC aan/uit	00	31	00	01-02
Auto.witbalans aan/uit	00	33	00	01-02

13. Toepassing

Hier kunt u taken in de videoserver automatiseren. De toepassingsconfiguratie bestaat uit 3 bereiken: gebeurtenis, server en medium. Een typisch toepassingsvoorbeeld kan er als volgt uitzien: op basis van een bewegingsherkenning (gebeurtenis) wordt een e-mail (server) naar een gebruiker met een alarmbeeld (medium) verzonden.

Gebeurtenis setup
Klik op **„Toevoegen"** om een nieuwe gebeurtenis in te stellen. Er kunnen maximaal 3 gebeurtenissen ingesteld worden.

„Gebeurtenisnaam" Geef een ondubbelzinnige naam waaronder u de gebeurtenisconfiguratie opslaat
„Gebeurtenis activeren" Kies de optie in om de geprogrammeerde gebeurtenis te activeren.
„Prioriteit" Gebeurtenissen met hogere prioriteiten worden eerst afgewerkt
„Vertraging" Pauzetijd tussen uitgevoerde gebeurtenissen (bijv.: bij bewegingsherkenning)

Event Settings

Event name:
Enable this event
Priority: Normal
Detect next event after 10 second(s).
Note: This can only applied to motion detection and digital input

Trigger
Video motion detection
Periodically
Digital input
System boot
Recording notify
Camera tampering detection
Video loss
IP changed
Video restore

Event Schedule
Sun Mon Tue Wed Thu Fri Sat
Time
Always
From 00:00 to 24:00 [hh:mm]

Gebeurtenisnaam: ABUS

Deze gebeurtenis inschakelen

Prioriteit: Normaal

Volgende gebeurtenis detecteren na 10 seconde(n).

NB: dit is alleen van toepassing op bewegingsdetectie en digitale ingang

Trigger

- Video bewegingsdetectie
- Periodiek
- Digitale ingang
- Systeemstart
- Opnamewaarschuwing
- Camera manipulatiedetectie
- Videoverlies
- IP is veranderd
- Video restore

Tijdschema gebeurtenissen

Zo Ma Di Wo Do Vr Za

Tijd

Altijd

Van 00:00 tot 24:00 [hh:mm]

Actie

Trigger digitale uitgang voor 1 seconden

Sauvegarde média si le réseau est débranché

Verplaatsen naar voorkeurspositie:

NB: s.v.p. configureren Presetlocaties eerste

Server toevoegen Media toevoegen

	Server	Media	
	SD	-----None-----	SD test Weergev
	NAS	Snapshot	Maak mappen automatisch
			Aangepaste map %Y%M%D/%H
			Weergev

13.1 Instellingen activering

„Videobewegingssensor” Activeer het gewenste bewegingsvenster
„Interval” De gebeurtenis wordt periodiek geactiveerd. Maximale instelling is 999 minuten
„Digitale ingang” Is er een signaal aan de alarmingang (bijv.: deurcontact), wordt er geactiveerd
„Systeemherstart” Gebeurtenis wordt bij het herstarten van de videoserver geactiveerd (tijdelijk spanningsverlies)
„Opnamealarm” Is het doelgeheugen (medium) vol of wordt een ringgeheugen overschreven, wordt een alarm geactiveerd.
„Camera sabotagebewaking” Er wordt een alarm geactiveerd als een camerasabotage van de aangesloten analoge camera herkend wordt.

„Videoverliesalarm” Er wordt een alarm geactiveerd als het videosignaal uitgevallen is.
„IP gewijzigd” Zodra aan een videoserver een nieuw IP-adres toegewezen wordt, wordt een alarm geactiveerd.
„Videosignaal hersteld” Is het videosignaal na een storing opnieuw voorhanden, wordt het alarm geactiveerd.

Gebeurtenistijdschema

„**Zon**” - „**Zat**” kiest de weekdagen voor de uitvoering van een gebeurtenis.
„**Altijd**” Activeert de gebeurtenis bij elke tijd (24 uur)
„**Van**” - „**tot**” De gebeurtenis is in de tijd beperkt.

13.2 Serverconfiguratie

Er kunnen 5 servers in de netwerkcamera opgeslagen worden. Klik op **„Toevoegen”** om een nieuwe server te configureren. De server van het type **„SD”** is vooringesteld en geeft de SD-kaarteenheid als doel voor gegevensopslag aan. De volgende servertypes kunnen geconfigureerd worden:

- E-mail: voer hier de toegangsgegevens in
- FTP: voer hier de toegangsgegevens in. Adresconventie: ftp.abus-sc.com
- HTTP: voer hier de toegangsgegevens in. Adresconventie: http://abus-sc.com/cgi-bin/upload.cgi
- Netwerkmap: Adresconventie: \\192.160.0.5\NAS

Servernaam:
Servertype
E-mail:
E-mail adres afzender:
E-mail adres ontvanger:
Serveradres:
Gebruikersnaam:
Wachtwoord:
Serverpoort 25
Voor deze server is een beveiligde verbinding vereist (SSL)
FTP:
HTTP:
Netwerkopslag:
Test Opslaan Sluiten

Na het invoeren van de toegangsgegevens moeten de instellingen opgeslagen worden. Voor u het venster sluit, is het aan te raden om een **„test”** uit te voeren. In een nieuw venster van de browser wordt het resultaat weergegeven.

13.3 Media-instellingen

Er kunnen 5 media-instellingen in de videoserver opgeslagen worden.

Medianaam: ABUS

Mediatype

Snapshot

Bron: Stream1

Verzenden 1 afbeelding(en) vóór de gebeurtenis [0~7]

Verzenden 1 afbeelding(en) na de gebeurtenis [0~7]

Bestandsnaam voorvoegsel:

Tijd en datum toevoegen aan de bestandsnaam

Videofragment

Systeemlog

Custom Message

Opslaan Sluiten

„Medianaam" Ondubbelzinnige naam voor het medium.

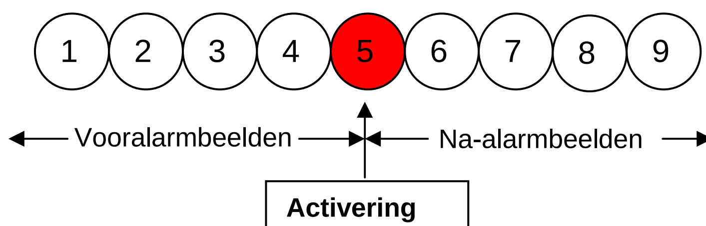
Er bestaan 4 verschillende mediatypes:

- Momentopname (bestandsformaat JPEG)
- Videoclip (bestandsformaat MP4)
- Logbestand (bestandsformaat TXT)
- Gebruikersgedefinieerde mededeling (bestandsformaat TXT)

Elk aangelegd medium mag alleen met een gebeurtenis verbonden worden.
Een dubbele bezetting van een medium heeft een incorrecte werking van de videoserver tot gevolg.
Wilt u voor twee gebeurtenissen hetzelfde mediatype gebruiken, dan moeten voordien ook twee afzonderlijke mediatypes aangelegd zijn.

Momentopname

„Bron" De opname kan van videostream 1 – 4 gebeuren
„Zend vooralarmbeelden" Aantal momentopnames voor een gebeurtenis
„Zend na-alarmbeelden" Aantal momentopnames na een gebeurtenis



„Bestandsnaamaanvulling" Voer hier een benaming in die vóór de bestandsnaam voor de momentopname geplaatst wordt.
„Datum en tijd aan bestandsnaam hangen" Met deze optie wordt de opgenomen momentopname van de datum en de tijd voorzien om de bestandsnamen van de momentopnames ofwel in het sequentiële of gebeurtenisgestuurde bedrijf makkelijk van elkaar te kunnen onderscheiden. Bijvoorbeeld betekent „video@20030102_030405.jpg" dat het JPEG-beeld op 2 januari 2003 om 3 uur, 4 minuten en 5 seconden opgenomen werd. Werd deze suffix weggelaten, dan wordt het bestand met de benaming „video.jpg" bij de externe ftp-server na het opgegeven tijdsinterval geactualiseerd

De bestandsnaam is als volgt opgebouwd:
Aanvulling_YYYYMMDD_HHMMSS : ABUS_20091115_164501

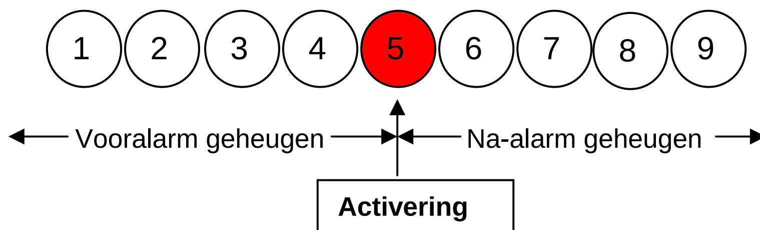
- Aanvulling: zie bestandsnaamaanvulling
- Y: plaatshouder voor jaar, YYYY = 2009
- M: plaatshouder voor maand, MM = 11
- D: plaatshouder voor dag, DD = 15
- H: plaatshouder voor uur, HH = 16
- M: plaatshouder voor minuut, MM = 45
- S: plaatshouder voor seconde, SS = 01

Videoclip

„Bron" De opname kan van videostream 1 – 4 gebeuren.

De videostream wordt als bron aangeboden die onder „audio en video" voor „Videobuffer" geconfigureerd is..

„Vooralarmopname" Vooralarm opname-interval in seconden (max. 9 seconden)
„Maximale duur" Maximale duur per bestand (max. 10 seconden)



„Maximale bestandsgrootte" Maximale grootte van het bestand in kByte (max. 800 kByte)
„Bestandsnaamaanvulling" Voer hier een benaming in die vóór de bestandsnaam voor de momentopname geplaatst wordt (details zie momentopname)

Logbestand
Slaat de actuele system-loginhoud in een tekstbestand op.

Custom Message
Een gebruikersgedefinieerde melding in de vorm van een tekstbestand wordt mee verzonden.

13.4 Actie

Actie

Trigger digitale uitgang voor 1 seconden

Sauvegarde média si le réseau est débranché

Verplaatsen naar voorkeurspositie:

NB: s.v.p. configureren Presetlocaties eerste

Server toevoegen | Media toevoegen

	Server	Media	
☐	SD	-----None-----	SD test · Weergev
☑	NAS	Snapshot	Maak mappen automatisch

Aangepaste map %Y%M%D/%H

Weergev

Configureer hier de actie die uitgevoerd moet worden als een geactiveerd alarm voorhanden is.
„Digitale uitgang actief voor" Bij activering wordt de relaisuitgang van de videoserver geschakeld.
„Ga naar positie" Er wordt een presetpositie bij alarm aangestuurd

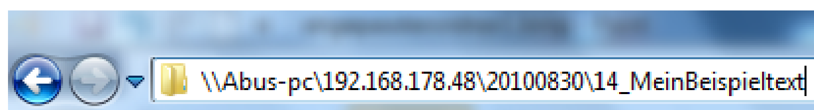
„**Server**” Bij een bepaalde server wordt het geselecteerde medium verzonden (bijv.: een e-mail wordt met een momentopname verzonden).

„Map automatisch aanmaken” Maakt automatisch een map in de directory van het netwerkloopwerk aan
„Aangepaste map” Met behulp van variabelen wordt de specifieke benaming van de map vastgelegd.
De ter beschikking staande variabelen vindt u in de onderstaande tabel terug.

Symbool	Voorbeeld/functie
/	*Nieuwe submap aanleggen*
%IP = IP-adres	*192.168.0.1*
%N = Eventname	*Motion_W1*
%Y = jaar	*2010*
%M = maand	*03*
%D = dag	*04*
%H = uur	*14*
„_Voorbeeldtekst”	*„_Voorbeeldtekst”*

Voorbeeld:
De volgende invoer zou dit pad aanmaken.

Maak mappen automatisch
Aangepaste map
%IP/%Y%M%D/%H_MeinBeispieltext
Weergev



13.5 Toepassingsoverzicht

Hier ziet u alle in de videoserver ingestelde „gebeurtenissen”, „mediatypes” en „servers”.
U kunt hier de verschillende instellingen controleren, wissen en nieuwe toevoegen.
Bovendien kunnen verschillende parameters, zoals bijv. naam, status, activering, standplaats, adres gecontroleerd worden.

Gebeurtenisinstellingen

Naam	Status	Zo	Ma	Di	Wo	Do	Vr	Za	Tijd	Trigger
ABUS	ON	V	V	V	V	V	V	V	00:00~24:00	boot

Toevoegen | ABUS | Wissen | Help

Serverinstellingen

Naam	Type	Adres/locatie
NAS	ns	\\my_nas\disk\folder

Toevoegen | Wissen

Media-instellingen

Beschikbare geheugenruimte: 9550KB

Naam	Type
Snapshot	snapshot

Toevoegen | Wissen

14. Opname

Het bereik opname dient om opnames in te stellen met het verschil dat hier permanente video-opnames voor SD-kaart of netwerkvrijgaven ingesteld kunnen worden. Twee opname-instellingen kunnen in de videoserver opgeslagen worden. Maak een nieuwe opname aan door een klik op **„Toevoegen"**

Naam van de opname: Video

Deze opname inschakelen

Prioriteit: Normaal

Bron: Stream1

Trigger

Tijdschema

Network fail

Tijdschema opname

Zo Ma Di Wo Do Vr Za

Tijd

Altijd

Van 00:00 tot 24:00 [hh:mm]

Bestemming SD

NB: Configureer s.v.p. om een opnamewaarschuwing te ontvangen Toepassing eerste

Doel: **„netwerkloopwerk"**

Bestemming NAS

Capaciteit:

Volledige lege ruimte

Gereserveerde ruimte: 15 Mbytes

Bestandsnaam voorvoegsel:

Maak mappen automatisch

Aangepaste map : %IP/%Y%M%D/%H

Cyclische opname inschakelen

NB: Configureer s.v.p. om een opnamewaarschuwing te ontvangen Toepassing eerste

Opslaan Sluiten

„Opname naam" Een ondubbelzinnige naam voor een opname-entry.
„Opname activeren" Vinkje plaatsen om de opname te activeren.
„Prioriteit" De opname met hogere prioriteit wordt prioritair uitgevoerd.
„Bron" De opname kan van videostream 1 – 4 gebeuren.
„Tijdschema" De opname tijdschema wordt gebruikt
„Netwerkfout" Treedt er een netwerkfout op, dan wordt de gegevensopslag automatisch op SD-kaart geactiveerd
„Zon" – **„Zat"** kiest de weekdagen voor de uitvoering van de opname.
„Altijd" Activeert de opname op elk moment.
„Van" – **„tot"** De opname is in de tijd beperkt.
„Doel" SD-kaart of netwerkmap

„Totale geheugenplaats” De maximaal op het doelgeheugen ter beschikking staande geheugenplaats wordt gebruikt.
„Gereserveerde plaats” Geeft aan hoeveel MB vrije geheugenplaats gereserveerd moet worden.
„Activeer ringgeheugen” Schakelt de ringgeheugenfunctie in. Wordt bij de gegevensopslag de ingestelde waarde bereikt, worden de oudste gegevens overschreven.

Voor meer aanwijzingen bij „Map automatisch aanmaken” gelieve naar hoofdstuk „13.4 Actie” te gaan.
Bij de geactiveerde functie "Aangepaste „map” kan de ringgeheugenfunctie niet gebruikt worden.

Opname-overzicht

„Naam (video)” Opent de opnameconfiguratiepagina
„Status (ON)” Zet de status van de opname op AAN/UIT
„Doel (SD)” Opent een detaillijst met de opgeslagen opnames

Opname-instellingen

Naam	Status	Zo	Ma	Di	Wo	Do	Vr	Za	Tijd	Bron	Bestemming
ABUS	ON	V	V	V	V	V	V	V	00:00~24:00	stream1	SD

Toevoegen | SD test | ABUS | Wissen

15. Lokaal geheugen

Dit hoofdstuk verklaart hoe het lokale geheugen (SD-kaart) van de videoserver beheerd kan worden. Er worden kaarten van het type SD/SDHC Class 6 tot 32GByte ondersteund.

Beheer van de SD-kaart

SD kaartbeheer

SD kaartstatus: Gereed

Totale omvang:	3860600 KBytes	Vrije afmeting:	3607712 KBytes
Gebruikte grootte:	252888 KBytes	Gebruik (%):	6.550 %

Formatteren

SD kaartbesturing:

☐ Cyclische opslag inschakelen

☐ Automatische schijfopruiming inschakelen

Maximale tijdsduur voor het bewaren van bestanden: 7

dagen

Opslaan

Gebruik de **„Formaat”**-functie als u de kaart voor de eerste keer in de videoserver inzet

Schakelt u de optie **„Overschrijven activeren”** in, dan worden de oudste bestanden eerst overschreven als de geheugencapaciteit van de SD-kaart bereikt is.

Activeert u de optie **„Automatisch wissen"**, dan wordt na het invoeren van de maximale verblijftijd de SD-kaart compleet gewist.

Zoeken en weergeven van de opnames
Wordt er geen criterium gekozen, dan worden altijd alle opnames in de resultatenlijst weergegeven.

Zoeken en de records inzien

Bestandsattributen:

Triggertype:	Digitale invoer	Videoverbinding verbroken	Video restore
	Systeemstart	Opnamewaarschuwing	Beweging
	Periodiek	Netwerkfout	IP is veranderd
	Sabotage		
Mediatype:	Videofragment	Snapshot	Tekst
Geblokkeerd:	Geblokkeerd	Blokkering verwijderd	

Triggertijd:

Van: Datum Tijd
tot: Datum Tijd
(yyyy-mm-dd) (hh:mm:ss)

Zoeken

„Activeringstype" Selecteer één of meerdere criteria, aan de hand waarvan een opname op de SD-kaart plaatsvond.
„Activeringstijd" Kies de gewenste periode

Klik op „Zoeken". Alle op de criteria van toepassing zijnde opnames worden in de gebeurtenislijst weergegeven.

Gebeurtenislijst e

Aantal elementen op een pagina

Zoekresultaten

Show 10 entries Search: — Zoeken

	Triggertijd	Mediatype	Triggertype	Geblokkeerd
☐	2010-09-09 13:54:40	Snapshot	Periodiek	Nee
☐	2010-09-09 13:54:40	Snapshot	Periodiek	Nee
☐	2010-09-09 13:54:40	Snapshot	Periodiek	Nee

Showing 1 to 3 of 3 entries — Pagina's ombladeren

Weergever | Downloaden | Alle markeringen wissen | JPEG's naar AVI | Blokkeren/vrijgeven | Verwijderen

„Weergeven" Geeft de geselecteerde opname in een nieuw venster weer.
„Download" Biedt de gekozen opname als download aan.

„JPEG naar AVI” Meerdere JPEG-beeldopnames kunnen geselecteerd worden (keuzebox) en worden in een AVI-bestand omgezet.
„Vergrendelen/ontgrendelen” Individuele opnames worden vergrendeld. Vergrendelde opnames worden niet door de cyclische opslag overschreven. Ontgrendelen verwijdert dit attribuut opnieuw.
„Verwijderen” Gekozen opname wordt gewist

U kunt alternatief ook de op de SD-kaart opgeslagen gegevens via uw SD-kaartlezer aan uw pc-systeem evalueren. De opgenomen gegevens worden conform de bestandsextensie met datum en tijd in de bestandsnaam weergegeven.

16. Logbestand

Klik op deze link op de configuratiepagina om het systeemprotocolbestand weer te geven. De inhoud van het bestand levert nuttige informatie over de configuratie en de verbinding na het starten van het systeem. De standaard van het logbestand is RFC 3164. U kunt eveneens gegevens naar een logserver sturen. Activeer hiervoor de optie „Remote protocol” en voer het IP-adres en het poortnummer van de server in.

17. Parameterlijst

Klik op deze link op de configuratiepagina om alle parameterrecords van het systeem weer te geven. Deze informatie kan voor support ter beschikking gesteld worden.

18. Beheer

Herstarten

Instellingen voor het opnieuw opstarten van de camera

Opmerking: Wanneer u de sequentie modus selecteert, dan start de camera na 24 uur na N dag(en)

Opnieuw opstarten

Sequentie mode :

Iedere 1 [1~30] Dag(en)

Tijdsplanning modus :

Zo Ma Di Wo Do Vr Za

Tijd 00:00 [hh:mm]

Opslaan | Nu opstarten

Opslaan | Nu opstarten

Herstellen

Alle instellingen terugzetten op de fabrieksinstellingen behalve de instellingen in

☐ Netwerktype ☐ Zomertijd

Herstellen

Bestanden exporteren

Configuratiebestand zomertijd exporteren | Export

Uitvoerinstellingen voor het back-up bestand | Export

Bestanden uploaden

Regels voor zomertijd bijwerken | Durchsuchen... | Upload

Uploadinstellingen voor het back-up bestand | Durchsuchen... | Upload

Firmware bijwerken

Kies bestand met firmware | Durchsuchen...

Bijwerken

Systeemherstart
Druk op de knop „Nu opnieuw starten" om de videoserver opnieuw te starten. U kunt alternatief een automatische toestelherstart configureren. Dit kan bij netwerkproblemen nuttig zijn. We raden u bij problemen aan om de videoserver wekelijks eens opnieuw te starten.

Herstellen
Druk op de knop om de voorinstellingen af fabriek te herstellen. Alle tot nu toe ingevoerde instellingen gaan hiermee verloren.

Bestand exporteren
Druk op de knop om uw videoserverinstelling in een bestand te exporteren. Ook kan het zomertijdconfiguratiebestand geëxporteerd en opgeslagen worden.

Bestandsupload
Druk op „Doorzoeken..." en kies het passende configuratiebestand.
Daarna drukt u op „uploaden" en wacht u tot de instellingen hersteld werden.

Firmware-update
Hier is het mogelijk om analoog met de update met de installatieassistent de firmware van de videoserver op de nieuwste stand te brengen. De actueelste firmware is op www.abus-sc.com verkrijgbaar. Kies het updatebestand (*.pkg) en druk op de knop UPDATE. De update neemt een korte tijd in beslag. Na de daaropvolgende herstart van de videoserver wordt deze met de nieuwe firmware in werking gesteld.

Koppel de videoserver in geen geval van de stroom los tijdens een firmware-update. Er bestaat gevaar voor onherstelbare schade.
Een firmware-update kan tot 10 minuten duren .

19. Onderhoud en reiniging

19.1 Werkingstest

Controleer regelmatig de technische veiligheid van het product, bijv. beschadiging van de behuizing.

Als aan te nemen is dat een veilig gebruik niet meer mogelijk is, dan moet het product buiten bedrijf gesteld worden en tegen het per ongeluk in gebruik nemen beveiligd worden.

Er dient vanuit gegaan te worden dat een veilig gebruik niet meer mogelijk is als

- het toestel zichtbare beschadigingen vertoont,
- het toestel niet meer functioneert en
- na langere opslag onder ongunstige omstandigheden of
- na zware transportbelastingen.

Het product is voor u onderhoudsvrij. Er zijn geen voor u te controleren of te onderhouden bestanddelen binnenin dit product, open het nooit.

19.2 Reiniging

Reinig het product met een schone droge doek. Bij sterke vervuiling kan de doek met lauw water bevochtigd worden.

Zorg ervoor dat er geen vloeistoffen in het toestel dringen, hierdoor zou het toestel vernietigd worden. Gebruik geen chemische reinigers, daardoor zou het oppervlak van de behuizing aangetast worden.

20. Afvalverwijdering

Toestellen die zo gemarkeerd zijn, mogen niet met het gewone huisvuil meegegeven worden. Voer het product op het einde conform de geldende wettelijke bepalingen af. Gelieve contact op te nemen met uw handelaar of voer de producten via het gemeentelijke verzamelpunt voor elektrisch afval af.

21. Technische gegevens

Typenummer	TVIP40000
Cameratype	Videoserver
Resolutie	QCIF,CIF,4CIF,D1 176x144 - 720x576 (tussenstappen vrij te kiezen)
Beeldelementen (totaal)	720x576
Beeldelementen (effectief)	720x576
Digitale zoom	4 x
Beeldcomprimering	H.264, MPEG-4, MJPEG
Beeldsnelheid	H.264 720X480@30FPS, 720x576@25FPS
	MPEG-4 720X480@30FPS, 720x576@25FPS
	MJPEG 720X480@30FPS, 720x576@25FPS
Videonorm	PAL, NTSC
Aantal parallelle streams	4
Maximaal aantal users	10
Bewegingsherkenning	3 zones
Voor-/na-alarmgeheugen	Ja
Beeldoverlay	Datum, cameranaam, privézones
Alarmingang (NO/NC)	1
Schakeluitgang	1 (12VDC@400mA)
Audio	Audio-uitgang (speaker out), audio-ingang, 2-weg-audio
Alarmmelding	E-mail / FTP / HTTP-bericht / relaisuitgang / NAS station / SD-kaart
Ondersteunde browsers	Mozilla Firefox of Internet Explorer 6.x en hoger
Ondersteunde software	eytron VMS, ONVIF ondersteuning
SD-kaart	max. 32 GB (SD/SD-HC)
RS-485 aansluiting	ja
PTZ-protocollen	Pelco D, Pelco P, LiLin, Samsung scc643, DynaDome / SmartDome
Netwerkaansluiting	RJ-45 ethernet 10/100 Base-T met PoE
Netwerkprotocollen	IPv4, IPv6, TCP/IP, HTTP, UPnP, RTSP/RTP/RTCP, IGMP, SMTP, FTP, DHCP, NTP, DNS, CoS, QoS, SNMP, 802.1X
Codering	HTTPS SSLv3
Toegangsbeveiliging	IP-adresfilter, gebruikersnaam, paswoord, 3 rechtenniveaus
Spanningsvoeding	12 VDC ,24 VAC, 802.3af PoE
Stroomverbruik	Max. 5,0 watt
Bedrijfstemperatuur	0 °C ~ 55 °C
Afmetingen (b x h x d)	75 x 35 x 150 mm
Certificeringen	CE, RoHS, C-Tick

22. URL opdrachten

Wanneer een klant beschikt over een eigen website of applicatie voor beheer, kan de netwerkvideoserver/ videoserver eenvoudig met behulp van URL syntax worden geïntegreerd. In dit hoofdstuk wordt de externe HTTP gebaseerde API besproken. Zie de appendix voor een volledig overzicht van de URL opdrachten.

23. Licentie informatie

Wij willen er op wijzen dat de netwerkvideoserver TVIP40000 onder andere Linux broncode bevat die valt onder de GNU General Public Licence (GPL). In overeenstemming met de GPL licentie van de gebruikte broncode verwijzen wij hierbij naar de licentievoorwaarden van GPL.

Licentietekst

De volledige tekst van de GNU General Public Licence is beschikbaar op de meegeleverde software CD of op de website van ABUS Security-Center onder http://www.abus-sc.de/DE/Service-Downloads/Software?q=GPL

Broncode

De gebruikte broncode is beschikbaar op de website van ABUS Security-Center onder http://www.abus-sc.de/DE/Service-Downloads/Software?q=GPL en is vrij beschikbaar voor download.

Werking van het volledige systeem

Door het downloaden van de software (broncodes) is het niet mogelijk om een volledig werkend systeem op te bouwen. Hiervoor is aanvullende software en de netwerkvideoserver benodigd.

24. Verwijzingen technologische licenties

H.264, MPEG-4 AAC technologie

DIT PRODUCT IS GELICENSEERD ONDER DE H.264, MPEG-4 AUDIO PATENT LICENTIE. DIT PRODUCT MAG NIET WORDEN GEDECOMPILEERD, REVERSE-ENGINEERED OF GEKOPIEERD, MET UITZONDERING VAN DE PC SOFTWARE MAG ER EEN ENKELE KOPIE VOOR ARCHIVERING WORDEN GEMAAKT. ZIE HTTP://WWW.VIALICENSING.COMVOOR MEER INFORMATIE.

H.264, MPEG-4 Visual Technology

DIT PRODUCT IS GELICENSEERD ONDER HET H.264, MPEG-4 VISUAL PATENT PORTFOLIO VOOR PERSOONLIJK EN NIET-COMMERCIEEL GEBRUIK DOOR DE EINDGEBRUIKER VOOR (i) HET AANMAKEN (ENCODEN) VAN VIDEO IN OVEREENSTEMMING MET DE MPEG-4 STANDAARD ("MPEG-4 VIDEO") EN/OF (ii) HET DECODEREN VAN VIDEO DIE IS GECODEERD DOOR EEN EINDGEBRUIKER VOOR PERSOONLIJK EN NIET-COMMERCIEEL GEBRUIK EN/OF IS VERKREGEN VAN EEN VIDEOLEVERANCIER DIE BESCHIKT OVER EEN LICENTIE VOOR HET LEVEREN VAN MPEG-4 VIDEO. ER ZAL GEEN LICENTIE WORDEN GEGEVEN OF BEDOELD VOOR ENIG ANDER GEBRUIK. AANVULLENDE INFORMATIE INCLUSIEF GEBRUIK VOOR PROMOTIE, INTERN EN COMMERCIEEL GEBRUIK EN LICENTIERING IS BESCHIKBAAR VAN MPEG LA, LLC. ZIE HTTP://WWW.MPEGLA.COM.

AMR-NB standaard

DIT PRODUCT IS GELICENSEERD ONDER DE AMR-NB STANDAARD PATENT LICENTIE-OVEREENKOMST. MET BETREKKING TOT HET GEBRUIK VAN DIT PRODUCT, ZIJN DE VOLGENDE PATENTEN VAN DE LICENTIEGEVER MOGELIJK VAN KRACHT:
TELEFONAKIEBOLAGET ERICSSON AB: US PAT. 6192335; 6275798; 6029125; 6424938; 6058359. NOKIA CORPORATION: US PAT. 5946651; 6199035. VOICEAGE CORPORATION: AT PAT. 0516621; BE PAT. 0516621; CA PAT. 2010830; CH PAT. 0516621; DE PAT. 0516621; DK PAT. 0516621; ES PAT. 0516621; FR PAT. 0516621; GB PAT. 0516621; GR PAT. 0516621; IT PAT. 0516621; LI PAT. 0516621; LU PAT. 0516621; NL PAT. 0516621; SE PAT 0516621; US PAT 5444816; AT PAT. 819303/AT E 198805T1; AU PAT. 697256; BE PAT. 819303; BR PAT. 9604838-7; CA PAT. 2216315; CH PAT. 819303; CN PAT.

ZL96193827.7; DE PAT. 819303/DE69611607T2; DK PAT. 819303; ES PAT. 819303; EP PAT. 819303; FR PAT. 819303; GB PAT. 819303; IT PAT. 819303; JP PAT. APP. 8-529817; NL PAT. 819303; SE PAT. 819303; US PAT. 5664053. DE LIJST KAN REGELMATIG WORDEN BIJGEWERKT. EEN ACTUELE VERSIE VAN DE LIJST IS BESCHIKBAAR OP DE WEBSITE VAN DE LICENTIEGEVER ONDER HTTP://WWW.VOICEAGE.COM.

TVIP40000

Betjeningsvejledning

Version 10/2010

Original betjeningsvejledning på dansk. Opbevares til senere anvendelse!

Introduktion

Kære kunde!

Vi takker for købet af dette produkt.

Det opfylder kravene fra de gældende europæiske og nationale retningslinjer. Det er blevet dokumenteret, og de pågældende erklæringer og dokumenter ligger hos producenten (www.abus-sc.com).

For at vedligeholde denne tilstand og for at sikre en risikofri drift skal du som bruger følge denne betjeningsvejledning!

Læs hele betjeningsvejledningen grundigt igennem, inden du tager produktet i brug.

Ved spørgsmål bedes du rette henvendelse til din systemopretter eller forhandler!

Ansvarsfraskrivelse

Denne betjeningsvejledning er blevet udarbejdet med stor omhu. Hvis du alligevel skulle finde udeladelser eller unøjagtigheder, så meddel dem venligst til os på den adresse, der står på bagsiden af betjeningsvejledningen.
ABUS Security-Center GmbH hæfter ikke på nogen måde for tekniske og typografiske fejl og forbeholder sig retten til uden foregående annoncering at foretage ændringer på produktet og på betjeningsvejledningerne.
ABUS Security-Center hæfter ikke og er ikke ansvarlig for direkte indirekte følgeskader, som opstår i forbindelse med udstyret, ydelsen og anvendelsen af dette produkt. Der gives ingen garanti for indholdet af dette dokument.

Symbolforklaring

Symbolet med en blitz i en trekant anvendes, hvis der er sundhedsfare, f.eks. gennem elektriske stød.

Et udråbstegn i en trekant gør opmærksom på vigtige oplysninger i denne betjeningsvejledning, som skal overholdes.

Dette symbol kan ses, hvis der er særlige tips og oplysninger med henblik på betjeningen.

Vigtige sikkerhedsoplysninger

Ved skader, som opstår pga. tilsidesættelse af denne betjeningsvejledning, bortfalder garantikravet. Vi hæfter ikke for følgeskader!

Vi hæfter ikke for skader på ting eller personer, som opstår pga. ukorrekt anvendelse eller tilsidesættelse af sikkerhedsoplysninger. I sådanne tilfælde bortfalder alle garantikrav!

Kære kunde! De følgende sikkerheds- og fareoplysninger hjælper ikke blot med at beskytte dig, men også apparatet. Læs venligst de følgende punkter grundigt igennem:

- Der er ingen dele i produktet, der kræver vedligeholdelse. Desuden bortfalder tilladelsen (CE) og garantien ved åbning/afmontering.
- Et fald selv fra lav højde kan beskadige produktet.
- Dette apparat er udviklet til anvendelse indendørs.
- Til udendørsbrug skal du anvende et egnet beskyttelseskabinet.
- Monter produktet på en sådan måde, at apparatets billedoptager ikke udsættes for direkte sollys. Vær opmærksom på monteringsoplysningerne i det pågældende kapitel i denne betjeningsvejledning.

Undgå følgende problematiske omgivelser ved betjeningen:

- Våde omgivelser eller for høj luftfugtighed
- Ekstrem kulde eller varme.
- Direkte sollys
- Støv eller brændbare gasser, dampe eller opløsningsmidler
- kraftige rystelser
- kraftige magnetfelter, som f.eks. i nærheden af maskiner eller højtalere.
- Videoserver må ikke installeres på ujævne flader.

Generelle sikkerhedsoplysninger:

- Lad ikke emballagemateriale ligge! Plastikfolier/-poser, polystyrendele osv., kan være farlige for børn.
- Børn må af sikkerhedshensyn ikke bruge videoovervågningsvideoserver pga. smådele, der kan sluges.
- Stik venligst ikke nogen genstande ind i apparatet gennem åbningerne
- Anvend kun de af producenten oplyste ekstraapparater/tilbehørsdele. Tilslut ingen ikke-kompatible produkter.
- Vær opmærksom på sikkerhedsoplysningerne og betjeningsvejledningerne af de øvrige tilsluttede apparater.
- Inden ibrugtagningen af apparatet skal det kontrolleres efter skader. Hvis der er skader, må apparatet ikke tages i brug!
- Overhold grænserne for den i de tekniske data nævnte driftsspænding. Højere spændinger kan ødelægge apparatet og være til fare for din sikkerhed (elektriske stød).

Sikkerhedsoplysninger

1. Strømforsyning: Strømforsyning 110-240 VAC, 50/60 Hz **/** 12VDC, 1.5 A (med i leveringsomfanget)
   Brug dette apparatet kun på en strømkilde, som leverer den på mærkepladen oplyste netspænding. Hvis du ikke er sikker, hvilken strømforsyning der er hos dig, så kontakt din el-leverandør. Fjern apparatet fra netstrømforsyningen, inden du gennemfører vedligeholdelses- eller installationsarbejde.

2. Overbelastning
   Undgå overbelastning fra netstikdåser, forlængerledninger og adaptere, da dette kan føre til brand eller elektriske stød.

3. Rengøring
   Rengør apparatet kun med en fugtig klud uden stærke rengøringsmidler.
   Apparatet skal i den forbindelse fjernes fra el-nettet.

Advarsler

Inden den første ibrugtagning skal man være opmærksom på alle sikkerheds- og betjeningsoplysninger!

1. Vær opmærksom på de følgende oplysninger for at undgå skader på el-kabler og el-stik:
   - El-kabler og el-stik må ikke forandres eller manipuleres.
   - El-kablet må ikke bøjes eller drejes.
   - Når du fjerner apparatet fra el-nettet, må du ikke trække i el-kablet, men holde fast i stikket.
   - Vær opmærksom på, at el-kablet ligger så langt væk som muligt fra varmeapparater for at forhindre, at plastbeklædningen smelter.

2. Følg disse anvisninger. Tilsidesættelse af dem kan føre til elektriske stød:

   - Åbn aldrig kabinettet eller strømforsyningen.
   - Stik venligst ikke nogen metal- eller brandfarlige genstande ind i apparatet.
   - For at undgå beskadigelser pga. overspænding (eksempel tordenvejr) skal du venligst anvende en overspændingsbeskyttelse.

3. Fjern venligst defekte apparater omgående fra el-nettet, og informer din forhandler.

Kontroller ved en installation i et eksisterende videoovervågningsanlæg, at alle apparater er fjernet fra el-net- og lavspændingsstrømkredsen.

I tvivlstilfælde bør du ikke foretage monteringen, installationen og kabelføringen selv, men overlade det til en fagperson. Ukorrekt eller ikke-fagligt arbejde på el-nettet eller på husinstallationer er ikke kun farligt for dig, men også for andre personer.
Tilslut installationerne på en sådan måde med kabler, at el-net- og lavspændingskredse altid forløber adskilt fra hinanden og ikke er forbundet med hinanden på noget sted eller kan forbindes gennem en defekt.

Udpakning

Mens du pakker apparatet ud, skal du håndtere det med stor omhu.

Ved eventuelle skader af originalemballagen skal du først kontrollere apparatet. Hvis der er skader på apparatet, skal du sende det retur med emballagen og informere leveringsservicen.

Inhaltsverzeichnis

Korrekt anvendelse

Der findes en udførlig funktionsbeskrivelse i kapitel “4. Første idriftsættelse”.

Produktet må ikke blive fugtigt eller vådt. Videoovervågningsvideoserver må kun anvendes i tørre rum.

En anvendelse ud over det, der er blevet beskrevet for oven, kan bl.a. føre til, at produktet beskadiges. Enhver anden anvendelse er ikke ifølge bestemmelsen og medfører, at garantien bortfalder. Enhver hæftelse bortfalder. Det gælder også, hvis der er blevet foretaget ombygninger og/eller ændringer på produktet.

Læs hele betjeningsvejledningen grundigt igennem, inden du tager produktet i brug. Betjeningsvejledningen indeholder vigtige informationer i forhold til montering og betjening.

1. Leveringsomfang

D1 Netværks Videoserver
TVIP40000

Netadapter

Beslag

Kort vejledning

Software-cd
inklusiv betjeningsvejledning

2. Montering

Kontroller, at der i leveringsomfanget er alle de tilbehørsdele og artikler, som er opført på den forrige liste. Driften af videoserver kræver et Ethernet-kabel. Dette Ethernet-kabel skal opfylde specifikationerne af UTP-kategori 5 (CAT 5) og må ikke overskride en længde på 100 meter.

2.1 Strømforsyning

Inden du starter med installationen, skal du kontrollere, at netspændingen og videoservers nominelle spænding stemmer overens.

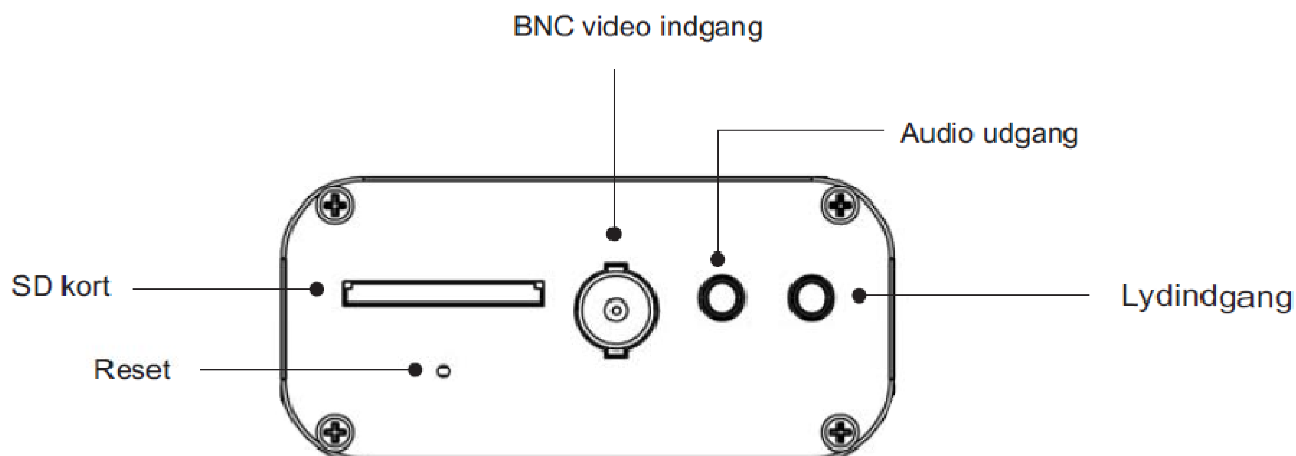
2.2 Montering af videoserver

Til vægmontagen af videoserveren er der brug for holdebøjlerne og skruerne, der findes i leveringsomfanget.

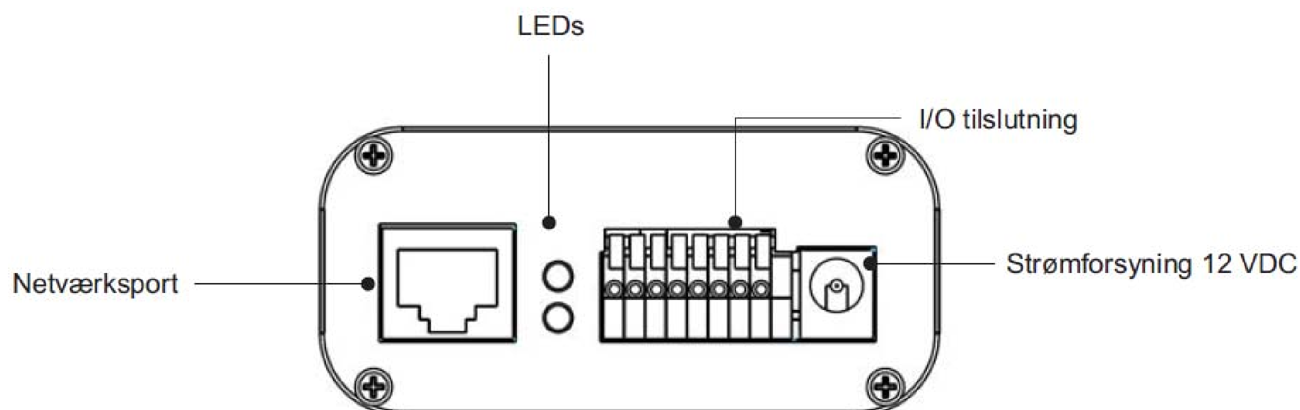
VIGTIGT !
Under monteringen skal videoserver været afbrudt fra netspændingen.

3. Beskrivelse af videoserver

3.1 Frontvisning

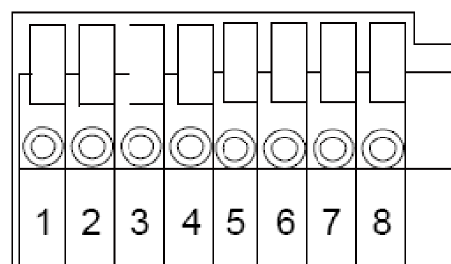


3.2 Bagsidevisning

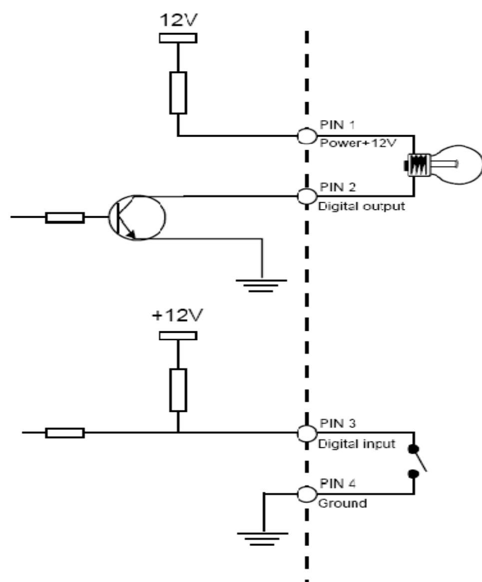


3.3 Alarmindgange og relæudgange

PIN	Beskrivelse
1	+12V udgang
2	Kontaktudgang
3	Alarmindgang
4	Masse
5	24V AC indgang
6	24V AC indgang
7	RS-485 +
8	RS-485 -



3.4 Kontaktind-/udgang og statusvisning



Blinkkode status-LED

Tilstand / LED-farve	Grøn	Rød
Systemstart	Fra	Til
Slukket	Fra	Fra
Netværkssøgning/-setup	1/s	Til
Netværksproblem	Fra	Til
Under firmware-opgradering	1/s	0.1/s
Indstil fabriksindstillinger	0.1/s	0.1/s

Anvend **Reset**-tasten for at nulstille netværksvideoservers indstillinger til tilstanden ved leveringen eller for at genstarte videoserver manuelt. Brug hertil et passende smalt værktøj.

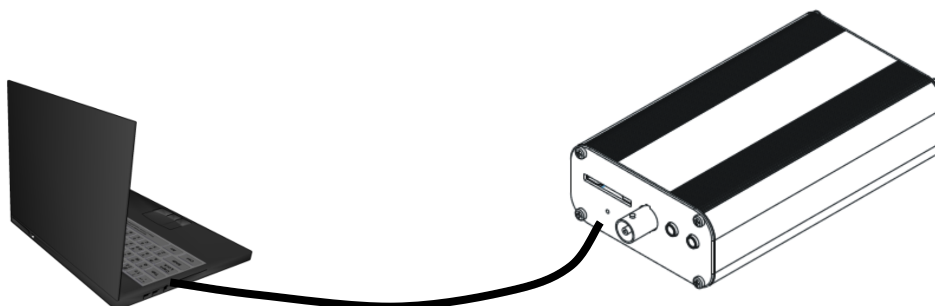
Genstart kamera: Tryk en gang på Reset-tasten, og vent, indtil videoserver igen er klar til brug.

Nulstil kamera: Tryk på Reset-tasten, og hold den nede i ca. 30 sekunder, indtil status-LED'en begynder at blinke. Alle indstillinger af netværksvideoserver nulstilles til tilstanden ved leveringen.

4. Første ibrugtagning

Direkte tilslutning af netværksvideoserver til en pc / laptop

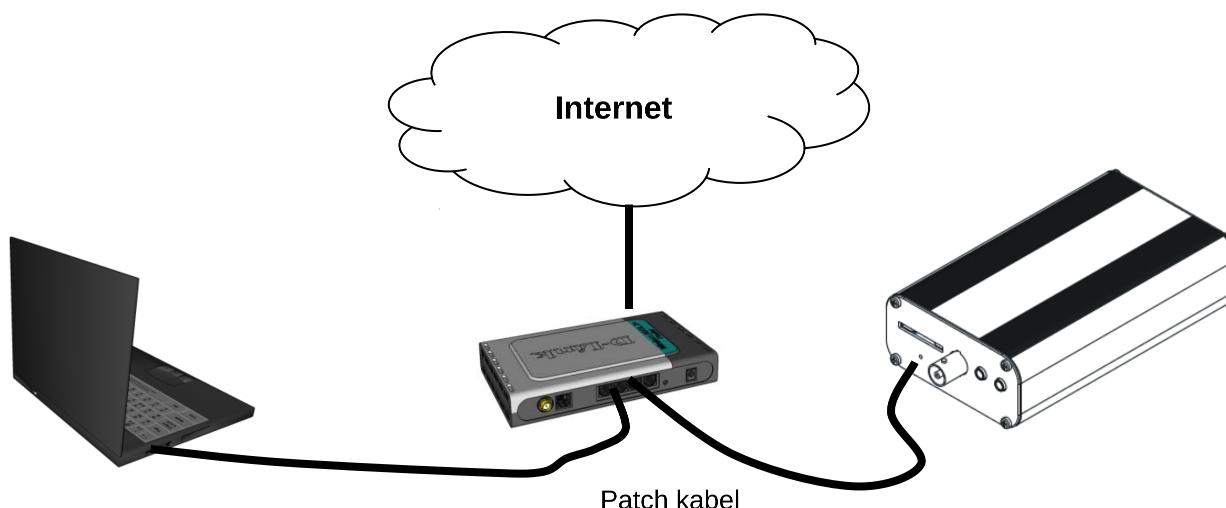
1. Kontroller, at du anvender et krydset netværkskabel (crossover)
2. Tilslut kablet til pc'ens / laptop'ens Ethernet-interface og netværksvideoserver
3. Tilslut netværksvideoservers spændingsforsyning
4. Konfigurer din pc's / laptop's netværksinterface til IP-adressen 169.254.0.1
5. Gå videre til punkt 5.1 for at afslutte den første opsætning og oprette forbindelsen til netværksvideoserver.



① krydset Ethernet-kabel

Tilslutning af netværksvideoserver til en router / switch

1. Kontroller, at du anvender et patch-kabel til netværket
2. Tilslut pc'en / laptop'en med router'en / switch'en.
3. Tilslut netværksvideoserver med router'en / switch'en.
4. Tilslut netværksvideoservers spændingsforsyning.
5. Hvis der i dit netværk er en navneserver (DHCP) til rådighed, skal du stille netværks-interfacet af din pc / laptop på „Hent IP-adresse automatisk“.
   Hvis der ikke skulle være nogen navneserver (DHCP) til rådighed, skal du konfigurere din pc's / laptop's netværksinterface til 169.254.0.1.
6. Gå videre til punkt 5.1 for at afslutte den første opsætning og oprette forbindelsen til netværksvideoserver.



4.1 Første adgang til netværksvideoserver

Den første adgang til netværksvideoserver sker ved anvendelse af Installationsassistent 2.
Efter start af assistenten søger denne efter alle tilsluttede EyseoIP-netværkskameraer og videoservere i dit netværk.

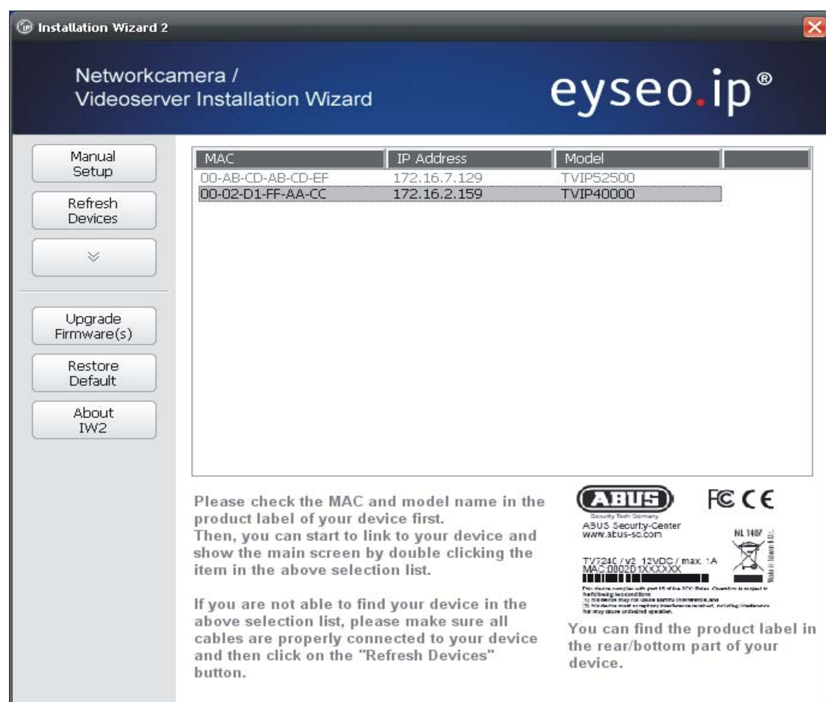
Du finder programmet på den vedlagte cd-rom under: **CD-ROM\Tools\EyseoIP Tools**

Installer programmet på dit pc-system, og udfør det. Installationsassistent 2 søger automatisk efter EyseoIP-netværkskameraer i dit netværk.

Netværksvideoservers standard-IP-adresse er **169.254.0.99**. Hvis du ikke anvender installationsassistenten, kan du få direkte adgang til videoserver, hvis dit pc-system er konfigureret til følgende adresseområde 169.254.0.1- 169.254.0.98.

Hvis der er en DHCP-server i dit netværk, sker tildelingen af IP-adresse automatisk, både for din pc / laptop og dit netværkskamera.

Start nu installationsassistenten. Hvis der ikke er nogen DHCP-server til rådighed, tilføjer installationsassistenten en virtuel IP-adresse fra området 169.1254.0.xx til din TCP/IP-konfigurering. Så længe installationsassistenten er åben, kan du via denne virtuelle IP-adresse oprette netværksadgang til videoserver. Vi anbefaler, at du omgående tilpasser videoservers netværkskonfigurering til det netværk, hvor videoserver skal anvendes.



Efter afslutning af Installationsassistent 2 fjernes den ekstra virtuelle IP-adresse igen. Hvis pc-systemets oprindelige IP-adresse ikke ligger i det samme IP-område som IP-videoserver er det ikke længere muligt at få adgang.

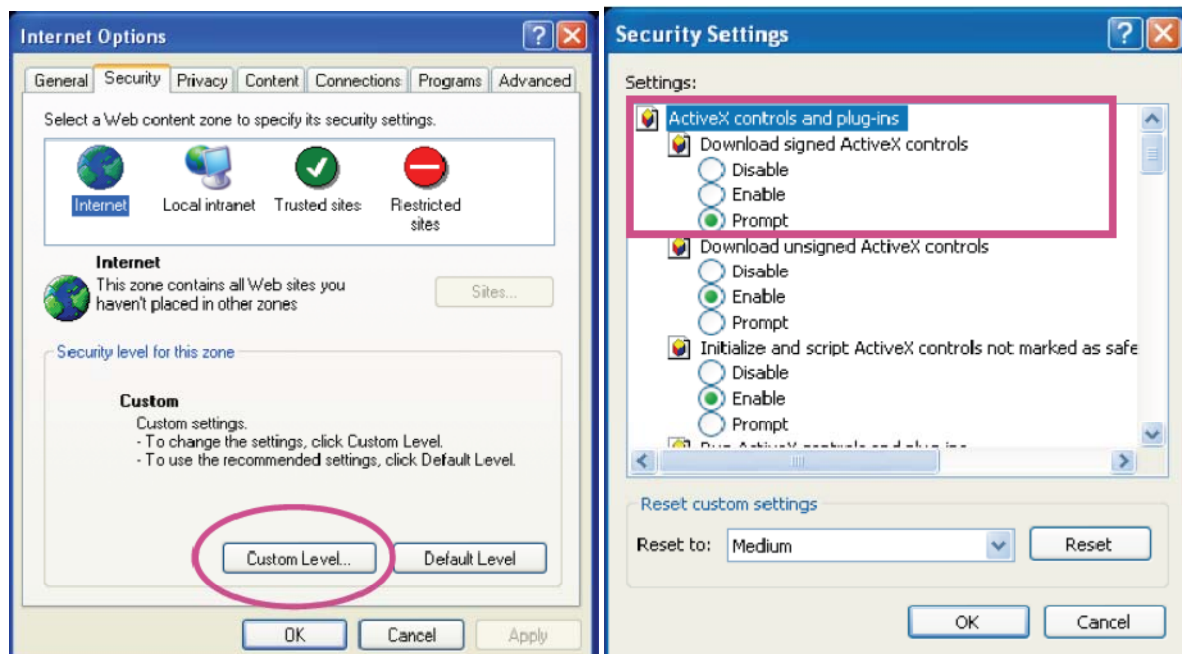
4.2 Adgang til netværksvideoserver via webbrowser

Ved den første adgang til netværksvideoserver i Windows spørger webbrowseren efter installationen af et ActiveX-plugin for netværksvideoserver. Denne forespørgsel afhænger af internet-sikkerhedsindstillingerne af brugerens pc. Hvis der er indstillet det højeste sikkerhedsniveau, kan computeren afvise enhver installation og hvert forsøg på en udførelse. Dette plugin anvendes til videovisningen i browseren. For at fortsætte kan brugeren klikke på „Installer“. Hvis webbrowseren ikke tillader at fortsætte installationen, skal du åbne internet-sikkerhedsindstillingerne og nedsætte sikkerhedsniveauet eller henvende dig til IT- eller netværksadministratoren.

4.3 Installer ActiveX-plugin

Hvis der til adgangen til videoserver anvendes browseren Mozilla Firefox eller Netscape, stilles der en Quick Time-stream til rådighed af videoserver i stedet for et ActiveX-plugin. Dette forudsætter, at du har Quick Time installeret på din computer.

4.4 Tilpasse sikkerhedsindstillinger



Bemærkning: Det kan ske, at din pc's sikkerhedsindstillinger forhindrer en videostream. Skift disse under punktet „Funktioner/Internetindstillinger/Sikkerhed“ til et lavere niveau. Vær især opmærksom på at aktivere ActiveX-objekter og -downloads.

4.5 Passwordforespørgsel

Fra fabrikken har netværksvideoserver ikke fået tildelt et administratorpassword. Af sikkerhedshensyn bør administrator straks fastlægge et nyt password. Efter lagringen af et sådant administratorpassword spørger netværksvideoserver inden hver adgang efter brugernavn og password.

Administratorens brugernavn er altid **„root"**, og dette kan ikke ændres. Efter ændringen af passwordet viser browseren et godkendelsesvindue og spørger efter det nye password. Efter indstillingen af passwordet er der ingen mulighed for at gendanne administrator-passwordet. Den eneste mulighed er at gendanne samtlige fabriksindstillede parametre.

For at indtaste et password skal du gøre som følger:

Åbn Internet Explorer, og indtast videoservers IP-adresse (f.eks. „http://192.168.0.99").

Du opfordres til at tilmelde dig:

-> Du er nu tilsluttet til netværksvideoserver og ser allerede en videostream.

4.6 Adgang til netværksvideoserver via RTSP-player

Du har mulighed for at få adgang til netværkets MPEG-4 datastrømme med en RTSP-egnet mediaplayer. Følgende gratis mediaplayer understøtter RTSP:

- VLC Media Player
- Real Player
- Quicktime Media Player

Adresseformatet for indtastningen af tilslutningsdata er opbygget som følger:

rtsp://<IP-adresse af netværksvideoserver>:<rtsp Port>/<Navn af videodatastrømmen>

Eksempel
rtsp://192.168.0.99:554/live.sdp

Nærmere oplysninger finder du i kapitlet „RTSP-overførsel".

4.7 Adgang til netværksvideoserver via mobiltelefon

Kontroller, at du kan oprette en internetforbindelse med din mobiltelefon. En anden forudsætning er, at dit apparat råder over en RTSP-egnet mediaplayer. Følgende mediaplayere for mobiltelefoner understøtter RTSP:

- Real Player
- Core Player

Vær opmærksom på, at adgangen til netværksvideoserver ved hjælp af en mobiltelefon kun er begrænset muligt pga. en formodentlig lav netværksbåndbredde. Vi anbefaler derfor følgende indstillinger for videostreamen for at reducere datamængden:

Videokomprimering	MPEG-4
Opløsning	176x144
Nøglebilledinterval	1 sekund
Videokvalitet (konstant bitrate)	40 Kbit / sekund
Audiokomprimering (GSM-AMR)	12.2 Kbit / sekund

Hvis din mediaplayer ikke understøtter RTSP-godkendelsen, skal du deaktivere godkendelsesmodus for RTSP i konfigureringsindstillingerne af netværksvideoserver.

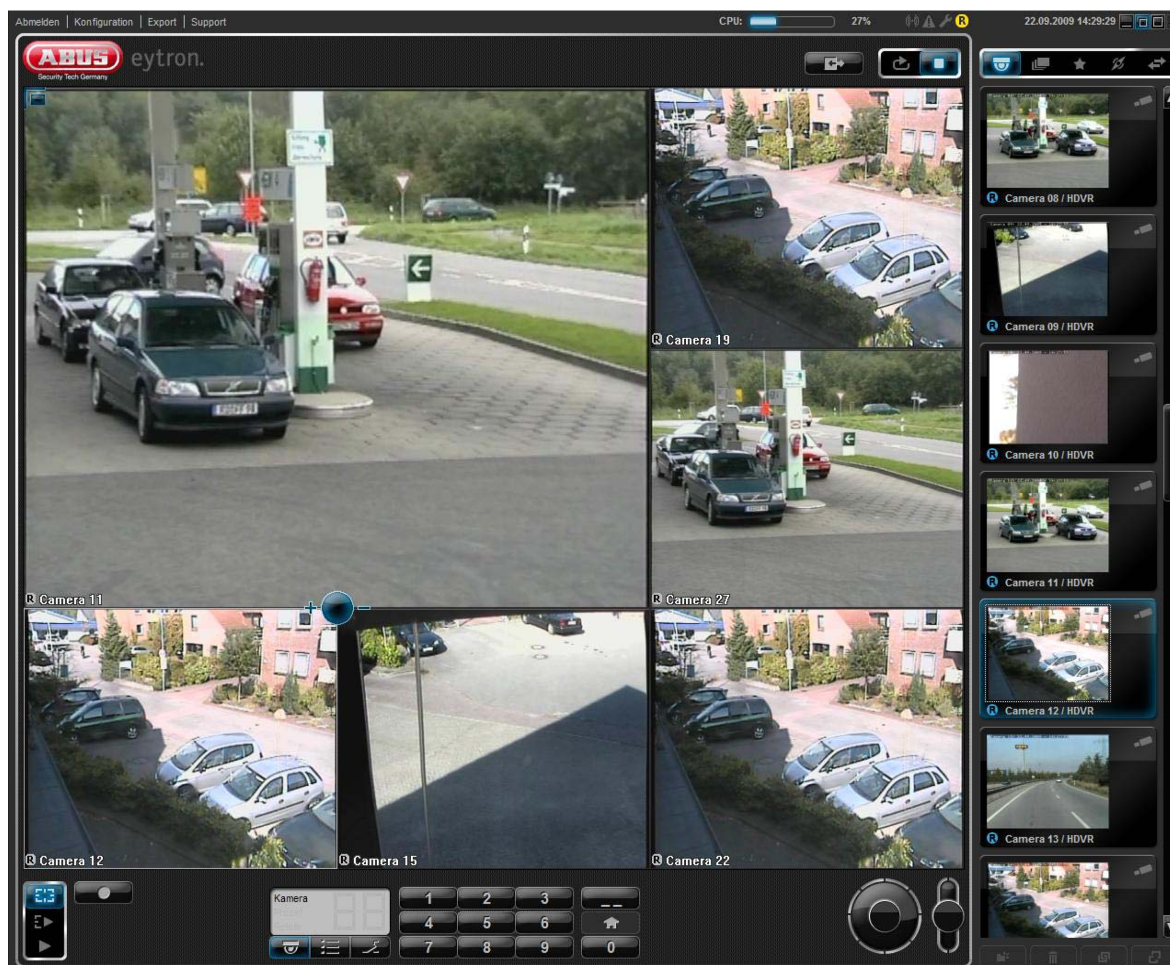
Adresseformatet for indtastningen af tilslutningsdata er opbygget som følger:

rtsp://<IP-adresse af netværksvideoserver>:<RTSP Port>/<Navn af videodatastrømmen>

Eksempel
rtsp://192.168.0.99:554/live.sdp

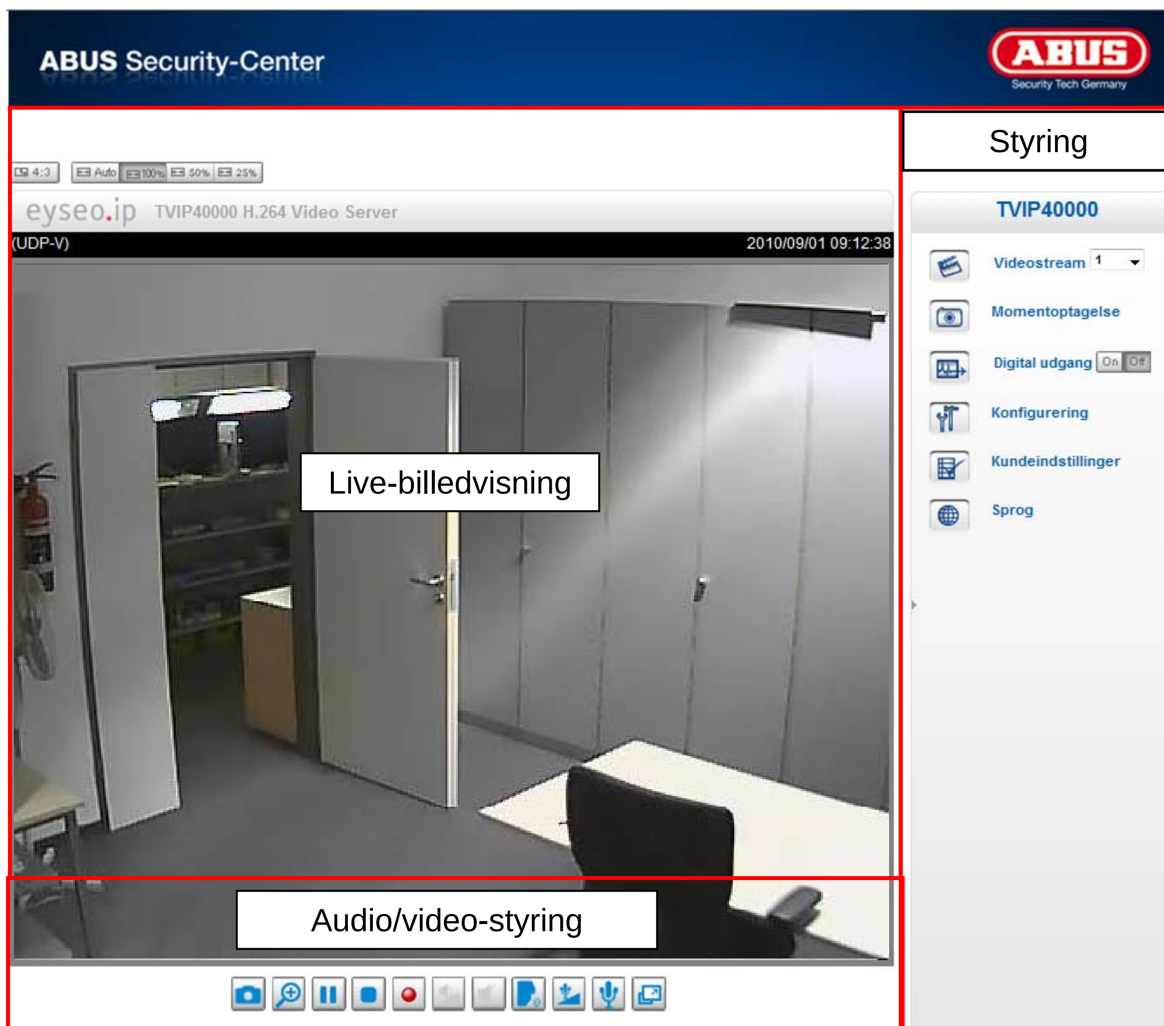
4.8 Adgang til netværksvideoserver via eytron VMS Express

På den cd-rom, der er med i leveringen, finder du den gratis optagelsessoftware eytron VMS Express. Hermed får du mulighed for at implementere og optage flere ABUS Security Center-netværkskameraer via én overflade. Yderligere oplysninger finder du i softwarens håndbog på den vedlagte cd-rom.



5. Brugerfunktioner

Åbn videoserverens startside. Overfladen er opdelt i følgende hovedområder:



Live-billedvisning

- Ændring af zoomtrinet ved at anvende musens scrollehjul
- Ved at klikke en gang på live-billedet kan du overtage styringen af et analogt pan/tilt kamera direkte.

Videoserverstyring

Videostream

Vælg mellem videostream 1-4 for live-billedvisningen

Momentoptagelse

Lav en momentoptagelse (uden ActiveX-plugin)

Digital udgang

Udgang, manuel til- og frakobling

Konfigurering

Gennemfør videoserverkonfiguration (administratorindstillinger)

Kundeindstillinger

Indstil kundeindstillingerne. Detaljer findes på de næste sider.

Sprog

Tilpas overfladens sprogindstilling

PTZ-styring

Anvend styrekontaktfladerne til digital og mekanisk PTZ-funktion

Tilpasset vinduesstørrelse

Hermed kan live-billedet tilpasses i 3 forskellige zoomtrin (100 %, 50 % og 25 %). Det er også muligt at tilpasse live-billedet automatisk til den aktuelle browserstørrelse. Hertil skal optionen “AUTO” vælges.

Skærmforhold

Med knappen “4:3” fastlægges live-billedets sideforhold til 4:3.

Åbn/luk menu

Med denne funktion kan menustyringen åbnes og lukkes.

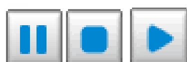
5.1 Audio/video-styring

Momentoptagelse

Webbrowseren viser et nyt vindue, hvor momentoptagelsen vises. For at gemme billedfilen på din pc skal du højreklikke på billedfladen og vælge optionen “Gem under”.

Digital zoom og momentoptagelse

Klik på lup-symbolet under videoserver-visningen. Derefter vises betjeningsfeltet for den digitale zoom. Deaktivér boksen “Deaktivér digital zoom”, og foretag ændring af zoomfaktoren med skydeknappen.

 Start/stop af live-billedvisningen

Live-stream’en kan efter ønske stoppes (standses) eller afsluttes. I begge tilfælde fortsættes der med play-symbolet i live-stream’en.

Lokal optagelse

Der kan startes eller stoppes en optagelse på den lokale harddisk. Optagelsesstien konfigureres under “Kundeindstillinger”.

Tilpas lydstyrken

Klik på symbolet for at indstille niveauet for audioudgangen manuelt.

Audio til/fra

Tale

Så længe der trykkes på kontaktfladen, overføres der audiosignaler fra pc'en til videoserverens audioudgang.

Mikrofon lydstyrke

Klik på symbolet for at tilpasse niveauet for videoserverens audioinddgang manuelt.

Mute

Slå videoserverens audioindgang til/fra.

Full screen

Aktivér full screen-visningen. Videoserverens live-billede vises, så det fylder hele skærmen.

5.2 Kundeindstillinger

Brugerindstillingerne gemmes på den lokale computer. Der står følgende indstillinger til rådighed:

Medieoptioner gør det muligt for brugeren at deaktivere audio- eller videofunktionen.

Protokoloptioner gør det muligt at vælge en forbindelsesprotokol mellem client og server. Der står to protokoloptioner til rådighed til optimering af programmet: UDP, TCP, HTTP.

UDP-protokollen et større antal audio- og videostreams i realtid mulig. Men nogle datapakker kan i den forbindelse mistes i netværket, fordi der forekommer mange data. Billeder kan derved kun gengives uklart. UDP-protokollen anbefales, hvis der ikke stilles specielle krav.

I TCP-protokollen mistes få datapakker, og en mere præcis videovisning garanteres. Men ulempen ved denne protokol består i, at stream'en i realtid er dårligere end den for UDP-protokollen.

HTTP-protokollen vælges, hvis netværket beskyttes med en firewall, og kun HTTP-porten (80) skal åbnes.

Valget af protokollen anbefales i følgende rækkefølge: UDP – TCP – HTTP

MP4 optagelsesoptioner: Gør det muligt for brugeren at tilpasse filstien til lagring af data med det samme. Kontaktfladen “Vedhæft dato og klokkeslæt til filnavnet” opretter filer med følgende identifikation:

CLIP_20091115-164403.MP4
Filnavn-tillæg_ÅrMånedDag-TimeMinutSekund.MP4

MP4 optagelsesoptioner
Mappe: c:\recordings Søger...
Filnavn-tilføjelse: CLIP
☑ Vedhæft dato og klokkeslæt til filnavnet
Gem

De optagede data kan afspilles med en MP4-egnet videoplayer (f.eks. VLC Mediaplayer).

6. Administratorindstillinger

6.1 System

Udelukkende administratoren har adgang til systemkonfigureringen. Hver kategori i den venstre spalte forklares på de følgende sider. Tekster med fed skrift udgør de specifikke oplysninger på optionssiderne. Administratoren kan indtaste URL'en under billedet for at komme direkte til billedsiden med konfigureringen.

ABUS Security-Center
ABUS Security Tech Germany

Konfigurering
- System
- Sikkerhed
- HTTPS
- SNMP
- Netværk
- DDNS
- Adgangsliste
- Video og Audio
- Bevægelsessensor
- Kamera sabotageregistering
- Kamerastyring
- Anvendelse
- Optagelse
- Lokal lagring
- Log-fi
- Parameterliste
- Administration

Version: 1210l

Home

System
Hostnavn: TVIP40000 H.264 Video Server
☐ Deaktiver belysning

Systemtid
Tidszone: GMT+01:00 Amsterdam, Berlin, Rome, Stockholm, Vienna, Madrid, Paris
☐ Aktiver sommertid:
Noter: Du kan uploade dine sommertids indstillinger på Administration siden eller bruge standart indstillingerne.
◉ Bibehold aktuel angivelse for dato og klokkeslæt
○ Synkroniser med pc tid
○ Manuel
○ Automatisk

DI og DO
Digital indgang: Normal status er Lav aktuel status **Høj**
Digital udgang: Normal status er Jordet aktuel status **Aben**

Gem

“Hostnavn” Teksten viser titlen på hovedsiden.

“Deaktiver belysning” Vælg denne option for at slukke videoserverens belysning. Hermed kan det forhindres, at andre personer kan konstatere videoserverens drift.

“Tidszone” Tilpasser klokkeslættet i overensstemmelse med den valgte tidszone.

“Aktiver sommertid” Aktiverer sommertidsindstillingerne i videoserveren. Alle sommertidsindstillinger for hver tidszone er allerede gemt i videoserveren.

“Bibehold aktuel angivelse for dato og klokkeslæt” Klik på denne option for at beholde videoserverens aktuelle dato og aktuelle klokkeslæt. Ved hjælp af et internt realtidsur bibeholdes videoserverens dato og klokkeslæt også efter et spændingstab.

“Synkroniserer med pc tid” Synkroniserer videoserverens dato og klokkeslæt med den lokale computer. Pc'ens skrivebeskyttede dato og skrivebeskyttede klokkeslæt vises efter aktualisering.

“Manuel” Indstiller datoen og klokkeslættet afhængigt af administratorens indtastning. Vær opmærksom på formatet i det pågældende felt ved indtastningen.

“Automatisk” Synkroniserer dato og klokkeslæt med NTP-serveren via internettet, når videoserveren startes. Dette sker ikke, hvis den tildelte tidsserver ikke kan nås.

“NTP-server” Tildeler tidsserverens IP-adresse eller domænebetegnelse. Hvis dette tekstfelt ikke udfyldes, forbindes videoserveren med standard-tidsserverne.

“DI og DO” Indstiller den fordefinerede tilstand for alarmindgang og relæudgang.

Glem ikke at klikke på **“Gem”**, så ændringerne aktiveres

6.2 Sikkerhed

“Root-password” Anvendes til at ændre administrator-passwordet ved at indtaste det nye password. De indtastede passwords vises af sikkerhedsmæssige årsager kun med prikker. Når der klikkes på **“Gem”**, opfordrer webbrowseren administratoren til at indtaste den nye password til adgang til videoserveren.

“Tilføj ny bruger” Indtast det nye brugernavn og det tilhørende password, og klik derefter på **“Tilføj”**. Den nye bruger vises på listen med brugernavnene. I alt kan der oprettes tyve brugerkonti.

“Rediger bruger” Åbn listen med brugernavnene, find brugeren, som du ønsker at redigere, og foretag ændring af de pågældende værdier. Klik på **“Opdater”** for at overtage ændringerne.

Root-password
Oplysning: Hvis der ikke er tildelt noget password, er systemet ikke beskyttet!
Root-password:
Bekræft root password:
Gem
Administrer rettigheder
Operatør
Seer
Digital udgang:
PTZ kontrol:
Tillad anonym visning
Gem
Brugeradministration
Eksisterende brugernavn:
--Tilføj ny bruger--
Brugernavn:
Bruger-password:
Bekræft brugerpassword:
Rettigheder:
Administrator
Slet
Tilføj
Opdater

"**Slet bruger**" Åbn listen med brugernavnene, find brugeren, og klik på **"Slet"** for at slette denne bruger fra listen

Brugeradministration

Administrator: Ubegrænset fuldstændig adgang til videoserveren.
Operatør: Ingen adgang til konfigureringssiden. Kan også udføre URL-kommandoer (f.eks. PTZ).
Seer: Adgangen er begrænset til hovedsiden (live-visning).

Digital udgang: Brugergruppen kan styre alarmindgang og udgang
PTZ kontrol: Brugergruppen har adgang til PTZ-styringen
Tillad anonym visning: Der spørges ikke om brugernavn og password, når hovedsiden vises.

6.3 HTTPS

HTTPS-protokollen anvendes til kodning og til autentificering af kommunikationen mellem webserver (videoserver) og browser (client-pc) i WWW. Alle data, der overføres mellem videoserver og client-pc, er kodet ved hjælp af SSL. Forudsætning for HTTPS er ud over SSL-kode (kompatibel med alle almindelige browsere) et certifikat, som bekræfter kildens autencitet.

Aktiver HTTPS
*Ved anvendelse af HTTP skal du først installere et certifikat!
Aktiver sikker HTTPS forbindelse:
HTTP & HTTPS Kun HTTPS
Gem
Opret certifikat
Opret selv-signeret certifikat automatisk
Opret selv-signeret certifikat manuelt:
Create certificate request and install:
Certifikat informationer
Status: Ikke installeret
Egenskaber Fjern

"Aktiver sikker HTTPS forbindelse" Efter ønske kan en ukodet (HTTP) + kodet (HTTPS) adgang eller udelukkende en kodet (HTTPS) adgang tillades.

Ved aktiv sikker HTTPS-forbindelse er der adgang til videoserveren via følgende linje:
https:\\"IP-adresse"
Anvend følgende link, hvis du vil streame via HTTPS-forbindelsen:
https:\\"IP-adresse":"HTTPS-port"\Live.sdp

Oprettelse og installation af certifikater

“Opret selv-signeret certifikat automatisk” Certifikatet, der er fordefineret i videoserveren, anvendes. Herved kan brugeren ikke foretage indstillinger.

“Opret selv-signeret certifikat manuelt” Der oprettes et nyt certifikat. Specifikke data skal indtastes.

“Opret og installer forespørgsel om certifikat” Med denne option kan der genereres en forespørgsel om certifikat, som kan oprettes på et certificeringssted. Der kan også installeres et certifikat, der er udstedt af et anerkendt certificeringssted (f.eks.: VeriSign), på videoserveren.

Anmærkning: Hvis du anvender et “selv-signeret certifikat”, modtager du evt. en advarselshenvisning fra browseren. Selv-signerede certifikater klassificeres af webbrowseren altid som usikre, da der hverken foreligger et stamcertifikat eller en dokumentation af autencitet fra et certificeringssted.

6.4 SNMP

Simple Network Management Protocol er en netværksprotokol til at kunne overvåge og styre netværksapparater (f.eks. router, server, switches, printer, computer osv.) fra en central station. Protokollen regulerer i den forbindelse kommunikationen mellem de overvågede apparater og overvågningsstationen. Aktiver denne funktion, når du anvender en SNMP-management-server i dit netværk. Du kan også gå tilbage til softwareløsninger, der kan installeres på dit pc-system.

“Aktiver SNMPv1, SNMPv2c” Afhængigt af indstillingerne af SNMP-serveren kan du her fastlægge skrive-/læsegruppernes navnefelter

SNMP Konfigurering

☑ Aktiver SNMPv1, SNMPv2c

SNMPv1, SNMPv2c Indstillinger

Læs/ skrive: Private

Læs kun: Public

☐ Aktiver SNMPv3

Gem

“Aktiver SNMPv3” Hvis SNMP-serveren understøtter SNMP-protokollen i version 3, kan du foretage statusforespørgslerne kodet. Hertil skal der for forespørgslen af skrive-/læsegrupperne gemmes en kodealgoritme og et password i videoserveren og SNMP-serveren.

6.5 Netværk

6.5.1 Netværksindstillinger

Alle ændringer, der foretages på denne side, medfører en genstart af systemet for at aktivere disse ændringer. Kontroller, at felterne er udfyldt rigtigt, før du klikker på “Gem”.

“LAN” Forindstillingen er LAN. Anvend denne indstilling, når videoserveren er forbundet med en LAN. Dertil er der brug for yderligere indstillinger som f.eks. IP-adresse og subnetmaske.

“Indstil IP-adresse automatisk” Ved hver genstart af videoserveren tildeles den en IP-adresse via en DHCP-server.

“Anvend fast IP-adresse” Netværksdataene som f.eks. IP-adressen tildeles her fast.

“**IP-adresse”** Der er brug for den til netværksidentificeringen.

“Subnetmaske” Den anvendes til at bestemme, om målet befinder sig i selve subnettet. Standardværdien er “255.255.255.0”.

“Standard-router” Det er gatewayen for videresendelse af billeder til et andet delnet. En ugyldig router-indstilling forhindrer overførslen til denne linje i forskellige delnet. Hvis der findes en cross-link-kabelforbindelse, skal der her ubetinget indtastes en IP i det samme subnetområde i videoserveren (f.eks. 192.168.0.1).

“Primær DNS” Den primære domænebetegnelses server, som hostnavnene omformes til IP-adresser med.

“Sekundær DNS” Den sekundære domænebetegnelses server til oprettelse af en reservekopi af den primære DNS.

“Anvend UPnP” Universal Plug and Play aktiveres hermed. Hvis operativsystemet understøtter UPnP, kan videoserveren aktiveres direkte via UPnP-forvaltningen (Windows: netværksomgivelser)

Sørg for, at optionen “Anvend UPnP” altid er aktiveret. UPnP anvendes også til at finde videoserveren for eytron VMS.

"UPnP portvideresendelse TIL" Universal Plug and Play-portvideresendelsen for netværkstjenester aktiveres hermed. Hvis routeren understøtter UPnP, aktiveres portvideresendelsen for videostream'en på routersiden automatisk for videoserveren med denne option.

"PPPoE" Anvend denne indstilling, når videoserveren er forbundet direkte med et DSL-modem. Brugernavn og password får du fra din ISP (Internet Service Provider).

"IPv6" Anvend denne funktion til at arbejde med IP-adresser i generation v6.

☑ Aktiver IPv6

IPv6 Information

☑ Manuel indstilling af IP adressen

Valgfri IP adresse / Prefix længde / 64

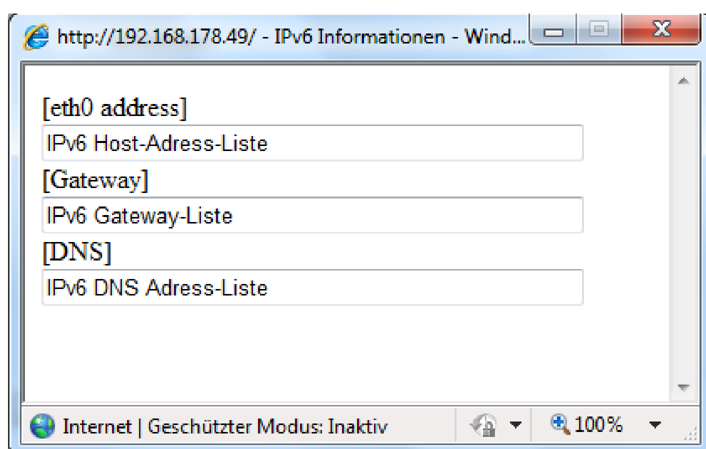
Valgfri default router

Valgfri primary DNS

Vær opmærksom på, at dit netværk og hardwaren skal understøtte IPv6.

Når IPv6 er aktiveret, venter videoserveren som standard, indtil routeren tildeler den en IPv6-adresse ved hjælp af DHCP.
Hvis der ikke findes en DHCP-server, skal du indstille IP-adressen manuelt.
Aktiver hertil "Manuel indstilling af IP adressen", og indtast IP-adressen, standard-routeren og DNS-adressen.

"IPv6 information" Alle IPv6-informationer vises et separat vindue.



Hvis IPv6-indstillingerne er korrekte, kan du aflæse alle indstillinger i det nederste vindue.

[eth0 address]

2001:0c08:2500:0002:0202:d1ff:fe04:65f4/64@Global

fe80:0000:0000:0000:0202:d1ff:fe04:65f4/64@Link

[Gateway]

fe80::211:d8ff:fea2:1a2b

[DNS]

2010:05c0:978d::

6.5.2 IEEE 802.1x

Aktiver denne funktion, når netværksomgivelserne anvender standarden IEEE 802.1x, en port-baseret adgangskontrol i netværket.
IEEE 802.1x forbedrer sikkerheden for lokale netværker.
En forbindelse tillades kun, når alle certifikater mellem server og “kunde” er blevet verificeret. Det sker via en autentificerer i form af et switch/access point, som sender forespørgsler til RADIUS autentificeringsserveren. I modsat fald etableres der ikke en forbindelse, og adgangen til porten blokeres.

Vær opmærksom på, at dine netværkskomponenter lige som RADIUS-serveren skal understøtte standarden IEEE 802.1x.

6.5.3 HTTP

“HTTP-port” Det kan være en anden port end den anførte port 80 (80 eller 1025 – 65535). Når porten er ændret, skal brugeren informeres om ændringen for at sikre, at der kan etalbleres en forbindelse. Hvis administratoren f.eks. ændrer HTTP-porten for videoserveren, hvis IP-adresse er 192.168.0.99, fra 80 til 8080, skal brugeren i stedet for “http://192.168.0.99” indtastes “http://192.168.0.99:8080” i webbrowseren.

“Sekundær HTTP-port” Ekstra HTTP-port til videoserveradgang

Til den direkte adgang til enkelte videostreams via web kan efterfølgende adgangsnavne indstilles. Adgangen foretages via komprimerede JPEG-billeder og gør den direkte adgang til videostream’en mulig for webbrowsere (Firefox, Netscape), der ikke kan bearbejde ActiveX-plugin:

“Adgangsnavn stream 1” Adgangsnavn for MJPEG-stream 1
“Adgangsnavn stream 2” Adgangsnavn for MJPEG-stream 2
“Adgangsnavn stream 3” Adgangsnavn for MJPEG-stream 3
“Adgangsnavn stream 4” Adgangsnavn for MJPEG-stream 4

Anmærkning: Internet Explorer understøtter ikke visning af MJPEG-billeder uden Active X

6.5.4 FTP

“FTP-port” Det er den interne FTP-server-port. Det kan være en anden port end den anførte port 21 (21 eller 1025 – 65535). Via FTP kan videodataene, der er gemt på videoserveren, hentes direkte. Anvend hertil et selvstændigt FTP-program.

Adresseformatet for indtastningen af forbindelsesdataene er opbygget på følgende måde:
Server: Videoserverens IP-adresse
Brugernavn: Administratorbruger
Password: Administratorens password
Port: Videoserverens FTP-port

Eksempel (med FTP-program)
Server: 192.168.0.99
Brugernavn: root
Password: admin
Port: 1026

Server: /mnt/auto/CF/NCMF

- /
  - mnt
    - auto
      - CF
        - NCMF
        - ncmf
    - CF

Dateiname /	Dateigröße	Dateityp	Zuletzt geändert	Berechtigu...	Besitzer/Gr...
000_1283513262.jpg	77.915	JPEG-Bild	03.09.2010 11:2...	-rwxr-xr-x	root root
000_1283513305.jpg	77.966	JPEG-Bild	03.09.2010 11:2...	-rwxr-xr-x	root root
000_1283513366.jpg	77.821	JPEG-Bild	03.09.2010 11:2...	-rwxr-xr-x	root root
000M.jpg	77.098	JPEG-Bild	03.09.2010 11:2...	-rwxr-xr-x	root root
001.jpg	77.218	JPEG-Bild	03.09.2010 11:2...	-rwxr-xr-x	root root
001M.jpg	77.259	JPEG-Bild	03.09.2010 11:2...	-rwxr-xr-x	root root
001M_1283513256.jpg	77.638	JPEG-Bild	03.09.2010 11:2...	-rwxr-xr-x	root root
001M_1283513303.jpg	78.269	JPEG-Bild	03.09.2010 11:2...	-rwxr-xr-x	root root
001M_1283513364.jpg	77.926	JPEG-Bild	03.09.2010 11:2...	-rwxr-xr-x	root root
002.jpg	77.267	JPEG-Bild	03.09.2010 11:2...	-rwxr-xr-x	root root
002_1283513268.jpg	78.236	JPEG-Bild	03.09.2010 11:2...	-rwxr-xr-x	root root
002_1283513310.jpg	78.411	JPEG-Bild	03.09.2010 11:2...	-rwxr-xr-x	root root
002_1283513368.jpg	77.496	JPEG-Bild	03.09.2010 11:2...	-rwxr-xr-x	root root
20100903_112614.mp4	542.681	MPEG-4 M...	03.09.2010 11:2...	-rwxr-xr-x	root root
20100903_112711.mp4	546.532	MPEG-4 M...	03.09.2010 11:2...	-rwxr-xr-x	root root
20100903_112819.mp4	547.002	MPEG-4 M...	03.09.2010 11:2...	-rwxr-xr-x	root root
normal-1283513308_2073467...	35.217.960	3GPP Movie	03.09.2010 11:2...	-rwxr-xr-x	root root
normal-1283513368_1099627...	2.565.197	3GPP Movie	03.09.2010 11:2...	-rwxr-xr-x	root root

19 Dateien und 2 Verzeichnisse. Gesamtgröße: 40.507.467 Bytes

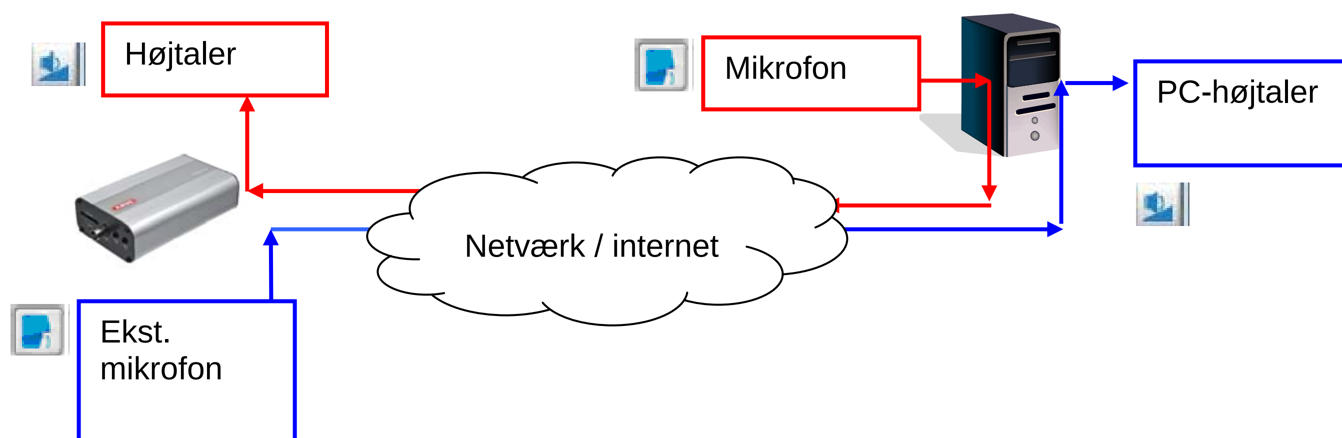
6.5.5 HTTPS

"HTTPS-port" Det er portindstillingen for den interne HTTPS-port. Det kan være en anden port end den anførte port 443 (443 eller 1025 – 65535). Yderligere indstillingsmuligheder for HTTPS findes under 5.5.3.

6.5.6 Tovejs-audio

"Tovejs-audio" Dette er porten funktionen tovejs-audio. Det kan være en anden port end den anførte port 5060 (5060 eller 1025 – 65535).

For at kunne anvende funktionen tovejs-audio skal du under **"Video og audio"** aktivere MPEG-4/H.264 for den valgte videostream. MJPEG understøtter udelukkende overførslen af videodata og er derfor ikke egnet til denne funktion.



Live-stream-funktioner:

Start overførslen af audiodataene.

Regulerer følsomheden for videoserverens audioindgang.

Slå mikrofonen/audioindgangen fra.

Klik på kontaktfladen igen for at standse audiooverførslen.

6.5.7 RTSP-overførsel

"RTSP-autentificering" Autentificeringen kan være disable (standard) eller Basic (enkel) eller udvidet mode (digest).

Hvis RTSP-autentificeringen er aktiveret, skal der indtastes et brugernavn og et password for en gyldig bruger ved etableringen af RTSP-forbindelsen (f.eks. administrator).
BEMÆRK: RTSP-autentificeringen skal understøttes af videoplayeren (f.eks. Realplayer 10.5).

"**Adgangsnavn for stream 1**" Dette er adgangsnavn 1 til at etablere en forbindelse fra en client. Codec-typen skal være MPEG4! Anvend
rtsp://<IP-adresse>:RTSP-port /<Adgangsnavn 1> for at etablere en forbindelse.

"**Adgangsnavn for stream 2**" Dette er adgangsnavn 2 til at etablere en forbindelse fra en client. Codec-typen skal være MPEG4! Anvend
rtsp://<IP-adresse>:RTSP-port /<Adgangsnavn 2> for at etablere en forbindelse.

"**Adgangsnavn for stream 3**" Dette er adgangsnavn 3 til at etablere en forbindelse fra en client. Codec-typen skal være MPEG4! Anvend
rtsp://<IP-adresse>:RTSP-port /<Adgangsnavn 3> for at etablere en forbindelse.

"**Adgangsnavn for stream 4**" Dette er adgangsnavn 4 til at etablere en forbindelse fra en client. Codec-typen skal være MPEG4! Anvend
rtsp://<IP-adresse>:RTSP-port /<Adgangsnavn 4> for at etablere en forbindelse.

RTSP-adgang med VLC:
rtsp://192.168.0.99:10052/live.sdp

"**RTSP-port**" Denne port kan afvige fra den forindstillede port 554 (554 eller 1025 til 65535). Vær ved ændring opmærksom på indtastningsformatet analogt med HTTP-porten.

"**RTP-port for video**" Denne port kan afvige fra den forindstillede port 5558. Portnummeret skal være et lige tal.

"**RTCP-port for video**" Denne port skal være "RTP-port for video" plus 1.

"**RTP-port for audio**" Denne port kan afvige fra den forindstillede port 5556. Portnummeret skal være et lige tal.

"**RTCP-port for audio**" Denne port skal være "RTP-port for audio" plus 1.

6.5.8 Multicast-overførsel

Multicast betegner en overførsel af beskeder fra et punkt til en gruppe (også kaldet flerpunktsforbindelse). Fordelen ved Multicast består i, at beskeder kan sendes samtidigt til flere deltagere eller til en lukket deltagergruppe uden, at båndbredden multipliceres med antallet af modtagere hos afsenderen. Ved multicasting skal afsenderen kun have den samme båndbredde som en enkelt modtager.
Pakken mangfoldiggøres på hver netværksfordeler (switch, router).

Multicast gør det muligt at sende data effektivt til mange modtagere samtidigt i IP-netværker. Det sker med en speciel Multicast-adresse. I IPv4 er adresseområdet 224.0.0.0 til 239.255.255.255 reserveret hertil.

Følgende Multicast-indstillinger kan konfigureres for stream 1 – 4 i videoserveren.

“**Altid Multicast**” Aktiver for at anvende Multicast.

“**Multicast gruppeadresse**” Specificerer en gruppe af IP-hosts, der hører til denne gruppe.

“**Multicast video-port**” Denne port kan afvige fra den forindstillede port 5560. Portnummeret skal være et lige tal.

“**Multicast RTCP video-port**” Denne port skal være “Multicast video-port” plus 1.

“**Multicast audio-port**” Denne port kan afvige fra den forindstillede port 5562. Portnummeret skal være et lige tal.

“**Multicast RTCP audio-port**” Denne port skal være “Multicast audio-port” plus 1.

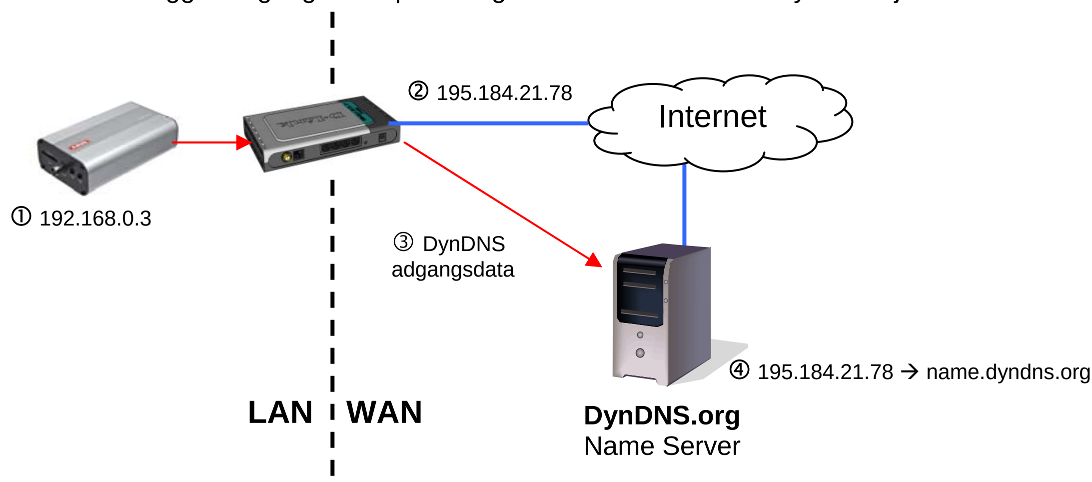
“**Multicast TTL**” time to live

Hvis du opretter en portvideresendelse i en router, skal alle ports altid videresendes (RTSP + HTTP). Dette er nødvendigt for at etablere kommunikationen.

7. DDNS

DynDNS eller DDNS (dynamisk domæne-navn-system-post) er et system, som kan opdatere domæne-navn-poster i realtid. Videoserveren har en integreret DynDNS-client, der automatisk kan opdatere IP-adressen hos en DynDNS-udbyder. Hvis videoserveren befinder sig bagved en router, anbefaler vi at anvendes routerens DynDNS-funktion.

Billedet anskueliggør adgangen til/opdateringen af IP-adressen hos DynDNS-tjenesten.



“**Aktiver DDNS**” Med denne option aktiveres DDNS-funktionen.

“**Udbyder**” Udbyderlisten indeholder hosts, som udbyder DDNS-tjenesteydelserne. Etabler en forbindelse med tjenesteudbyderens webside for at sikre, at tjenesteydelsen står til rådighed.

“**Hostnavn**” For at anvende DDNS-tjenesteydelsen skal dette felt udfyldes. Indtast hostnavnet, som er registreret på DDNS-serveren.

“**Brugernavn/e-mail**” Brugernavnet og e-mail-adressen skal indtastes i feltet for at etablere en forbindelse med DDNS-serveren eller for at informere brugerne om den nye IP-adresse. Henvisning: Hvis “brugernavnet” skal indtastes i dette felt, skal “passwordet” indtastes i det følgende felt.

“**Password**“ Indtast dit password her for at kunne anvende DDNS-tjenesteydelsen.

DDNS: Dynamic domain name service

Aktiver DDNS:

Udbyder: Dyndns.org(Dynamic)

Hostnavn:

Brugernavn:

Password:

Gem

7.1 Indstilling af DDNS-konto

Indstilling af ny konto ved DynDNS.org

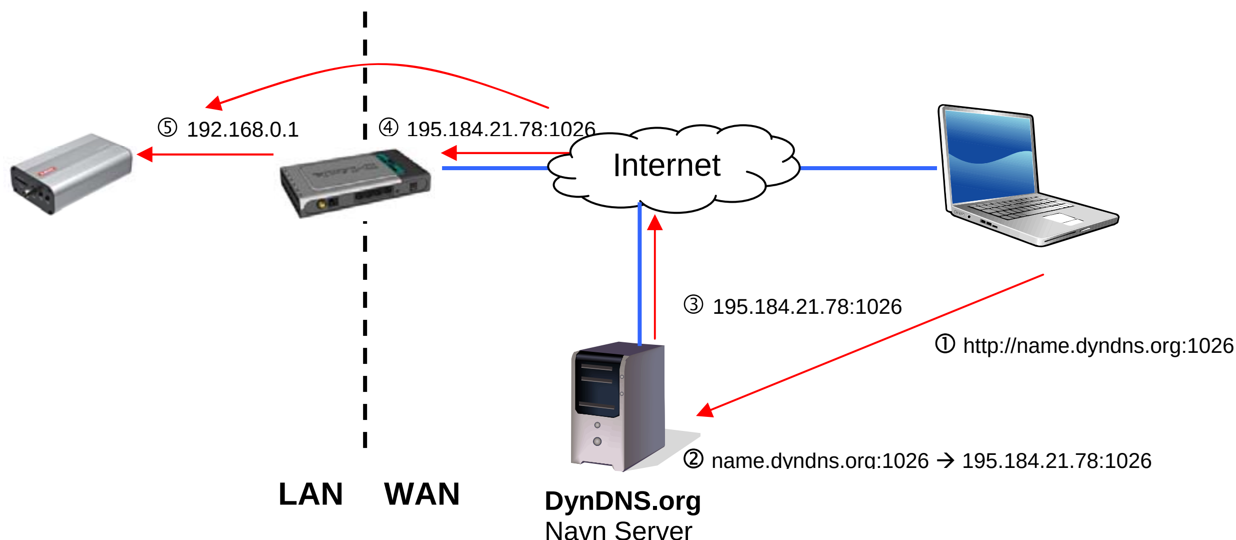
Lagring af account-informationer

Noter dine brugerdata, og overfør dem til videoserverens konfigurering

7.2 DDNS-adgang via router

Hvis netværksvideoserveren befinder sig bagved en router, skal adgangen via DynDNS konfigureres i routeren. Hertil findes der på ABUS Security-Center hjemmesiden www.abus-sc.com en beskrivelse til DynDNS-router-konfigureringen for almindelige router-modeller.

Følgende billede anskueliggør adgangen til en videoserver bagved en router via DynDNS.org.



For DynDNS-adgangen via en router skal der indstilles en portvideresendelse for alle relevante ports (mindst RTSP + HTTP) i routeren.

8. Adgangsliste

Her styres adgangene til videoserveren ved hjælp af IP-adresselister.

"Maksimal antal samtidige forbindels(er) er begrænset til" Antal af mulige samtidige adgange til videoserveren. Afhængigt af båndbredden, der står til rådighed for videoserveren, kan det være hensigtsmæssige at begrænse adgangen.
"Aktiver adgangsliste" Aktiverer IP-adressefiltrene, der er defineret under "Filter"

Du har to muligheder for at definere IP-adressefiltreringen.

- Filtertype "Tillad": Kun IP-adresser i det definerede adresserum har adgang
- Filtertype "Nægt": IP-adresser i det definerede adresserum har ingen adgang

Klik på "Tilføj" for at konfigurere adresseområderne. Der findes følgende indstillingsmuligheder:

Generelle indstillinger

Maksimal antal samtidige forbindels(er) er begrændset til: 10 Se Information

Aktiver adgangsliste filtrering

Gem

filter type

Tillad Nægt

Gem

Filter

IPv4 adgangs liste

Tilføj Slet

Administrator IP adresse

Tillad altid at IP addressen kan forbinde til enheden

Gem

Regel: Single, område, netværk:

- Single: Der tilføjes en specifik IP-adresse
- Område: Der kan defineres IP-adresseområder fra – til
- Netværk: Der kan defineres IP-adresser med specifik subnetmaske

Tilføj ipv4 filter listen

filter adresse

Regler: Single

Single
Netværk
Område

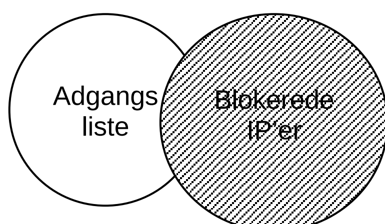
IP-adress

OK Afbryd

Eksempel:
IP-adresseområdet fra 192.168.0.1 til 192.255.255.255 skal tillades.
Følgende IP-adresser skal blokeres, 192.168.1.0 til 192.168.255.255

Resultat:
Der må kun foretages adgang fra IP'er fra følgende område: 192.168.0.1 – 192.168.0.255

Der dannes en fællesmængde mellem tilladte adgange og blokerede IP'er.



9. Audio og video

Home

Videoindstillinger

Videotitel:

Farve: Farve

Modulation: Auto

Vælg caching stream: Stream 4

Videoudretning: Hælde Spejl

Vis titel og timestamp i videobilledet.

Billedindstillinger Privatzonemaskering

Video kvalitets indstillinger for stream 1:

Video kvalitets indstillinger for stream 2:

Video kvalitets indstillinger for stream 3:

Video kvalitets indstillinger for stream 4:

Audio indstillinger

Lydløs

Mikrofonindgang: 0 dB

Audio type:

AAC:

AAC bit rate: 16 Kbps

GSM-AMR:

G.711:

Modus: pcmu

Gem

"Videotitel" Teksten vises i den sorte bjælke over videovinduet med et tidsstempel. Dette tidsstempel (dato og klokkeslæt) leveres af videoserverens integrerede realtidsur.

"Farve" Vælg mellem visning med farver eller i sort/hvid.

"Modulation" Vælg mellem videostandarden NTSC og PAL eller en automatisk registrering af videosignalet med videoserveren.

"Videobuffer" Den valgte videostream anvendes til optagelsen af for- og efteralarm-videodata (se afsnittet "Anvendelse").

"Hælde" Til at dreje videoen horisontalt. Vælg disse optioner, hvis kameraet blev installeret omvendt.

"Spejl" Til at dreje videoen vertikalt.

Anvend optionen Hælde + Spejl, når kameraet er installeret i loftet.

“Vis titel og timestamp i videobilledet” Med denne option kan titler og tidsstempler vises direkte i videobilledet og momentoptagelser. Indtastningen under punktet “Videotitel” anvendes her.

9.1 Billedindstillinger

“Lysstyrke, kontrast, mætning, skarphed”
Tilpas værdierne i overensstemmelse med lysforholdene.

Hvis du ændrer kameraets lysforhold, kan billedindstillingerne for dårlige lysforhold have en negativ påvirkning af billedkvaliteten ved gode lysforhold.

Klik på “Preview” for at vise de ændrede indstillinger for billederne. Klik på “Gem” for at overtage billedparametrene. Klik på “Gendan”, hvis du ikke ønsker at overtage ændringerne.

9.2 Privatzonemaskering

Med denne funktion kan områder i videobilledet skjules. Der kan maksimalt markeres 5 vilkårligt store områder.

Aktiver først denne funktion ved at sætte fluebenet ud for **“Aktiver privatzonemaskering”**.

Med kontaktfladen **“Ny”** oprettes et nyt vindue, størrelsen kan derefter tilpasses. Tryk på **“Gem”** for at overtage indstillingerne.

Denne funktion skal ikke aktiveres, når kameraets PTZ/ePTZ-funktion anvendes. Denne funktion kan kun konfigureres, når MS Internet Explorer anvendes som browser (ActiveX-mode).

9.3 Grundindstilling

Videooptioner

Videoserveren stiller af hensyn til den fleksible anvendelse fire videostreams til rådighed i forskellige opløsninger.

- Video kvalitets indstillinger for stream 1:
- Video kvalitets indstillinger for stream 2:
- Video kvalitets indstillinger for stream 3:
- Video kvalitets indstillinger for stream 4:

Indstillinger for streams 1, 2, 3 og 4
Med den pågældende menu konfigureres stream 1 – 4

Opløsningen ved stream 4 er fastlagt til QCIF. Anvend stream 4 til at streame på mobile apparater.

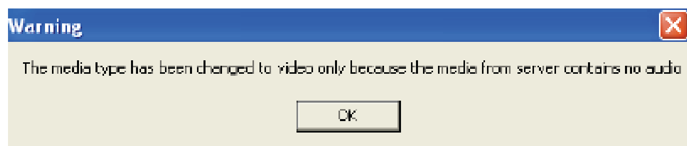
“Billedkomprimering” Vælg mellem H.264/MPEG-4/MJPEG.
“Billedstørrelse” Indstil den ønskede opløsning her.
“Maks. billedhastighed“ Indstil den maksimale billedgentagelseshastighed her.
“Nøglebilled-interval” Fastlægger, hvor ofte der oprettes en I-frame. Jo kortere intervallet er, desto bedre billedkvalitet opnås der, men på bekostning af højere belastning af netværket.
“Videokvalitet fast billedhastighed” Fastlægger billedhastighed konstant på en værdi. Billedkvaliteten falder ved tiltagende billedkompleksitet (f.eks.: bevægelse).
“Fast billedkvalitet” Fastlægger billedkvaliteten på en konstant værdi. Bitraten stiger ved tiltagende billedkompleksitet (f.eks.: bevægelse).

Komprimering → / Optagelsesvarighed ↓	**H.264**	**MPEG-4**	**MJPEG**
1 minut videosekvens i D1 opløsning med kvalitet “god”	Ca. **12** MB	Ca. **14** MB	Ca. **60** MB
Lagerkapacitet **32 GB** SD-kort	Ca. **43** timer	Ca. **36** timer	Ca. **9** timer

I slutningen af håndbogen findes en detaljeret tabel med hver kvalitetsindstilling kombineret med hver opløsning

9.4 Audio-indstillinger

"Lydløs" Alle audiofunktioner i videoserveren deaktiveres. Der vises en henvisning ved adgang til videoserveren



"Ekstern mikrofon/audioindgang forstærkning" Tilpas værdien fra +21 db til -33 db

"Audiotype" Vælg audiotypen og den ønskede bitrate her. En højere værdi kræver mere båndbredde:

- **"AAC"** (Advanced Audio Coding) Specielt codec til audiodatakomprimering under MPEG-4/H.264.
- **"GSM-AMR"** (Global System for Mobile Communications - Adaptive Multi Rate) Sprog-codec i GSM-mobilnettet.
- **"G.711"** pmca/pmcu (impulskodemodulation)

10. Bevægelsesgenkendelse

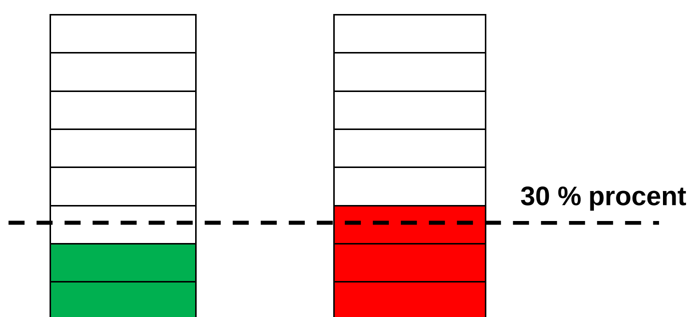
Der kan aktiveres indtil tre bevægelseszoner i videoserveren. Vælg **"Aktiver bevægelsesføler"** for at foretage konfigureringen.

Funktionen bevægelsesgenkendelse er først aktiv, når der er fastlagt en handling under menupunktet "Anvendelse".

"Vinduenavn" Teksten vises foroven i vinduet.
"Følsomhed" Følsomhed ved ændringer i billedforløbet (f.eks.: Høj følsomhed: Opløsning ved lav billedændring.
"Procent" Angiver, hvor procent af billedet der skal ændres, for at bevægelsesføleren udløser.

Klik på **"Ny"** på denne kontaktflade for at tilføje et nyt vindue. For at indstille vinduets størrelse igen eller at forskyde titelbjælken skal du klikke med den venstre musetast på vinduets ramme, holde den trykket ned og trække den til den ønskede størrelse med cursoren. Ved at klikke på 'x' i vinduets øverste højre hjørne slettes vinduet. Klik på "Gem" på denne kontaktflade for at gemme de tilsvarende indstillinger for vinduet. Afhængigt af billedvariationen stiger eller falder en grafikbjælke.

En grøn bjælke betyder, at billedvariationen befinder sig under overvågningsniveauet, mens en rød bjælke henviser til, at billedvariationen befinder sig over overvågningsniveauet. Hvis den røde bjælke vises, vises det registrerede vindue også med en rød kant. Ved at gå tilabge til startsiden skjules det overvågede vindue. Men den røde ramme vises, så snart der registreres en bevægelse.



Grønt område: Bevægelse blev registreret, men medførte ikke en alarmudløsning
Rødt område: Billedvariation (bevægelse) overstiger grænseværdien på 30 % og medfører en alarm.

Funktionsmåde ved bevægelsesgenkendelse:

Du har to parametre til at indstille bevægelsesgenkendelsen: **Følsomhed** og **Procent**. Billedet forklarer, hvordan disse to parametre påvirker bevægelsesgenkendelsen.

Fra billede A til billede B finder der en bevægelse sted. De resulterende pixelændringer (afhængigt af følsomhedsindstillingen) vises i billede C (grå). Indstillingen **"Følsomhed"** henviser til sensorikkens evne til at genkende bevægelser i billedet. Jo højere denne værdi er indstillet, desto flere pixelændringer genkendes der i billedet. Ved en bevægelsesgenkendelse gemmes pixelændringerne (afhængigt af følsomheden) serverinternt som alarmpixel (lyserøde felter i billede D). Tærskelværdien **"Procent"** beskriver i den forbindelse andelen af "alarmpixel" i forhold til det samlede pixelantal i det valgte område. Hvis den fastlagte andel af alarmpixel (procent) nås/overskrides, udløses der en alarm. For en pålidelig bevægelsesgenkendelse anbefales det at indstille en høj følsomhed og en lav procentværdi.

11. Kamera sabotageregistrering

Videoserveren understøtter en sabotageregistrering. Hvis registreringen er aktiveret, kan en resulterende alarm anvendes som resultat for en meddelelse (se anvendelse)

"Aktiver videoserver sabotageovervågning" Sensorikken aktiveres.

"Udløsningsreaktion" Tidsrummet definerer, hvor længe en sabotagehændelse skal foreligge, før der udløses en alarm.

Følgende sabotagehændelser kontrolleres:

- Kameradrejning
- Kameraafdækning
- Kameradefokussering

Denne sabotageregistrering kan du anvende som udløser i kamerafunktionen "Anvendelse/ hændelses-setup".

12. Kamerastyring

Videoserveren giver mulighed for at styre et analogt PTZ-kamera.

RS485-indstillinger

"Deaktiveret" RS485-styringen er frakoblet

"PTZ Kamera" Indtast de pågældende parametre for PTZ-kameraet her. Følgende protokoller understøttes: Pelco-D, Pelco-P, Samsung scc643, DynaDome/SmartDOME, Lilin PIH-7x00.
Hvis dit PTZ-kamera ikke understøtter en af disse protokoller, skal du vælge "Brugerdefineret kamera"

"Transparent HTTP Tunnel" Hvis dit PTZ-apparat understøtter RS485-kommandoer via et netværksinterface, kan du vælge denne option. De nødvendige parametre findes i betjeningsvejledningen for PTZ-apparatet.

RS485 indstillinger

Deaktivere
PTZ Kamera
Transparent HTTP Tunnel

Kamera ID: 1
PTZ driver: Pelco D protocol
Portindstillinger:
Baud rate: 2400
Databits: 8
Stopbits: 1
Paritet: ingen

Forudindstillede positioner | Brugerdefineret kommando

Gem

De nøjagtige PTZ-kommadoer findes i betjeningsvejledningen for PTZ-apparatet.

“Kamera ID” Fastlægger kameraets ID.
“PTZ driver” Fastlægger protokollen for det tilsluttede PTZ-apparat.
“Baud rate” Indstil den passende baudrate.
“Databits” I ndstil de passende databits.
“Stopbits” Indstil de passende stopbits.
“Paritet” Fastlægger pariteten.

Forudindstillede positioner og indstilling af patrulje

Der kan gemmes i alt 20 forudindstillede positioner i videoserveren. Gå frem på følgende måde:

1. Positioner kamerabilledet på den ønskede indstilling med retningstasterne
2. Giv den aktuelle position et forudindstillet navn, og klik på Tilføj. Navnet vises i listen med forudindstil-lede positioner
3. Gentag trinene 1 – 2 for andre forudindstillede positioner
4. Marker de forudindstillede positioner, som du vil anvende til en patrulje, og bekræft dem med “Vælg”
5. Tilpas om nødvendigt opholdstiden for den pågældende forudindstillede position.
6. Gem indstillingerne.

Tryk på “Patrol” i videoserverens live-billede for at starte patruljen. På “STOP” for at standse den

Brugerdefineret kommando

Menupunktet “Brugerdefineret kommando” muliggør direkte adgang til enkelte funktioner i PTZ-apparatet eller PTZ-kameraet.
Som regel anvendes funktionen til at hente gemte forudindstillede positioner eller fordefinerede patruljer.

Brugerdefineret kommando

Hvis du lader "Display visning" være tom, vises knappen ikke på hjemmesiden.

	Display visning	Kommando
Kommando 1:	Tour1	FF01000900010B
Kommando 2:		
Kommando 3:		
Kommando 4:		
Kommando 5:		

Gem Luk

Ved hjælp af denne funktion kan du oprette dine egne kommandokontaktflader i videoserverens live-billede til at betjene/indstille det tilsluttede PTZ-apparat.
Den pågældende funktion for kontaktfladen beskrives med en hexadecimalkode (afhængigt af den pågældende PTZ-protokol).
Alle ABUS Speeddome-kameraer anvender protokollerne PELCO D/P.
Der kan maksimalt oprettes 5 brugerdefinerede kontaktflader.
Under "kontaktfladenavn" skal du indtaste det ønskede navn på kontaktfladen (f.eks.: Patrulje 1).

Hvis du har indtastet "Brugerdefineret kamera" som kameraprotokol, skal du fastlægge grundlæggende funktioner som f.eks. "Op","Ned","Venstre","Højre" under "Brugerdefineret kommando". Koderne, der er ansvarlige herfor, findes i vejledningen til PTZ-apparatet.

Hvis der ikke angives et kontaktfladenavn, vises kontaktfladen ikke i live-billedet

Pelco D/P-protokollen arbejder udelukkende med hexadecimale tal.

Indtast HEX-koden for den ønskede funktion under “Kommando”.
(f.eks.: FF 01 00 09 00 01 0B**)**

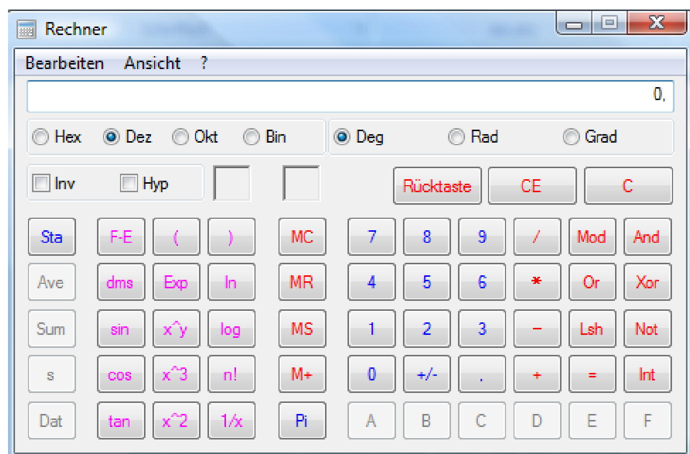
Koden må ikke indeholde mellemrum og specialtegn.
FF 01 00 09 00 01 0B → FF01000900010B

Forord hexadecimaltal
I følgende kapitel forklares det hexadecimale talsystem ved hjælp af et par eksempler.

Decimal	Hex	Decimal	Hex	Decimal	Hex
1	1	11	B	30	1E
2	2	12	C	40	28
3	3	13	D	50	32
4	4	14	E	60	3C
5	5	15	F	70	46
6	6	16	10	80	50
7	7	17	11	90	5A
8	8	18	12	100	64
9	9	19	13	500	1F4
10	A	20	14	1000	3E8

Det hexadecimale talsystem er baseret på tallene fra 0 til 9 og bogstaverne fra A til F. Når checksummerne beregnes, skal der tages højde for, at hexadecimal adderes.

En vigtig hjælp ved omregningen fra decimal til hexadecimal og addering af hexadecimal er lommeregneren, der er integreret i Microsoft Windows, og som hertil skal være indstillet på “Videnskabelig”.



Dome-styrekommandoer for TV7600,TV6702,TV7604 (Pelco)

Kommandosammensætning

Ord 1	Ord 2	Ord 3	Ord 4	Ord 5	Ord 6	Ord 7
Synch Byte (altid FF)	Address (ID for det analoge kamera)	Command 1	Command 2	Data 1	Data 2	Check Sum ord 2 – 6

Beregning checksum:

Ord 7 = ord 2 + ord 3 + ord 4 + ord 5 + ord 6

Worterklärung:

“Ord 1” Altid deklareret som „FF“
“Ord 2” Bestemmer det analoges kameras ID
“Ord 3” – “Ord 4” Fastlægger de forskellige PTZ-funktioner (“Gem forudindstillede positioner”, “Start patrulje” osv.)
“Ord 5” – “Ord 6” Fastlægger f.eks. nummereringen af de forudindstillede positioner og patruljer.
Hvis du vil køre til en forudindstillet position, skal det også fastlægges, hvilket forudindstillet nummer der skal køres til.
“Ord 7” er summen af ord 2 – ord 6 og kendes også som checksummen

Eksempel: “Gå til forudindstillet 1” har kommandoen: FF 01 00 07 00 **01** 09

Ord 1 er altid fastlagt til FF
Ord 2 er altid ID for speed-dome
Ord 3 og ord 4 bestemmer funktionen: “Gå til forudindstillet”
Ord 5 og ord 6 bestemmer, hvilken forudindstillet position der skal køres til.
Ord 7 checksum

Forklaring: I ord 6 står hextallet 01 for forudindstillet 1.
Hvis man nu ville køre til forudindstillet 15, måtte man skrive 0F i ord 6.

Eksempel: “Gå til forudindstillet 15” har kommandoen: FF 01 00 07 00 **0F** 17
Fremgangsmåde er analog med valget af patruljer eller andre funktionsstrukturer, der kan tælles.

Glem ikke at beregne checksummen igen efter hver ændring af kommandoen.
En ændring af kommandoen i ovenstående eksempel fra forudindstillet 1 til forudindstillet 15 ville medføre, at checksummen bliver 14 større!

Oversigt over kommandoer:

Kommando	Ord 3	Ord 4	Ord 5	Ord 6
Ned	00	10	00	2A
Op	00	08	00	3C
Drej til venstre	00	04	2E	00
Drej til højre	00	02	06	00
Stop	00	00	00	00
Menu	00	11	00	00
Start tour	00	00	09	01 til 08
Scan	00	0F	00	01
Zoom tele	00	20	00	01
Zoom wide	00	40	00	01
Focus near	01	00	00	01
Focus far	00	80	00	00
Iris close	04	00	00	00
Iris open	02	00	00	00
Gem forudindstillet	00	03	00	01 to C8
Slet forudindstillet	00	05	00	01 to C8
Gå til forudindstillet	00	07	00	01 to C8
Set Auxiliary	00	09	00	01 to 08
Clear Auxiliary	00	0B	00	01 to 08
Remote Reset	00	0F	00	00
Set Zone Start	00	11	00	01 to 08
Set Zone End	00	13	00	01 to 08
Write Char. To Screen	00	15	X position 00 til 28	ASCII Value
Clear Screen	00	17	00	00
Alarm Acknowledge	00	19	00	Alarm No.
Zone Scan til	00	1B	00	00
Zone Scan fra	00	1D	00	00
Indstil mønsterstart	00	1F	00	00
Indstil mønsterstop	00	21	00	00
Kør mønster ned	00	23	00	00
Indstil zoomspeed	00	25	00	00 to 03
Indstil Focus Speed	00	27	00	00 to 03
Kameraets fabriksindstilling	00	29	00	00
Autofokus auto/til/fra	00	2B	00	00-02
Auto iris auto/til/fra	00	2D	00	00-02
AGC auto/til/fra	00	2F	00	00-02
BLC til/fra	00	31	00	01-02
Auto. hvidjustering til/fra	00	33	00	01-02

13. Anvendelse

Her kan du automatisere opgaver i videoserveren. Anvendelseskonfigureringen består af 3 områder: Hændelse, server og medium. Et typisk anvendelseseksempel kan se på følgende måde: På grund af en bevægelsesgenkendelse (hændelse) sendes en e-mail (server) til en bruger med et alarmbillede (medium).

Hændelses-setup
Klik på **"Tilføj"** for at oprette en ny hændelse. Der kan maksimalt indstilles 3 hændelser.

"Hændelsesnavn" Giv et entydigt navn, som du gemmer hændelseskonfigureringen under
"Aktiver hændelse" Indstil optionen for at aktivere den programmerede hændelse.
"Prioritet" Hændelser med højere prioritet behandles først
"Forsinkelse" Pausetid mellem udførte hændelser (f.eks.: Ved bevægelsesgenkendelse)

Hændelsesnavn: ABUS

☑ Aktiver hændelse

Prioritet: Normal

Forsinkelse for 10 Sekund(er).

Oplysning: Dette kan kun anvendes for bevægelsesgenkendelse og digital indgang

Udløser

- Videobevægelsessensor
- Periodisk
- Digital indgang
- Systemgenstart
- Optagelses besked
- Kamera sabotageregistering
- Mistet video-alarm
- IP ændret
- Video restore

Hændelsestidsplan

☑ Søn ☑ Man ☑ Tir ☑ Med ☑ Tor ☑ Fre ☑ Lør

Tid

- Altid
- Fra 00:00 til 24:00 [hh:mm]

Handling

☐ Digital udgang aktiv for 1 Sekunder

☐ Back-up media wanneer de verbinding met het netwerk verbroken is

☐ Gå til preset position

Oplysning: Konfigurering Forudindstillede steder først

Tilføj server | Tilføj medie

	Server	Medie	
☐	SD	-----None-----	SD Test Se
☑	NAS	Snapshot	☐ Opret mapper automatisk
			Tilpassede mappe %IP/%Y%M%D/%H_MeinBeispieltext
			Se

Gem | Luk

13.1 Indstillinger for udløser

“Videobevægelsessensor” Aktiver det ønskede bevægelsesvindue
“Periodisk” Hændelsen udløses periodisk. Maksimal indstilling er 999 minutter
“Digital indgang” Hvis et signal er aktiveret på alarmindgangen (f.eks.: dørkontakt), udløses der
“Systemgenstart” Hændelse udløses, når videoserveren genstartes (midlertidigt spændingstab)
“Optagelsesbesked” Hvis mållageret (medium) er fuldt, eller hvis et ringlager overskrives, udløses en alarm.
“Kamera sabotageregistrering” Der udløses en alarm, hvis der registreres en kamerasabotage på det tilsluttede analoge kamera.
“Mistet video-alarm” Der udløses en alarm, hvis videosignalet mistes.
“IP ændret” Så snart videoserveren tildeles en ny IP-adresse, udløses der en alarm.
“Video restore” Hvis videosignalet foreligger igen efter en fejl, udløses der.

Hændelsestidsplan

"**Søn**" – "**Lør**" vælger ugedagene for udførelsen af en hændelse.
"**Altid**" Aktiverer hændelsen på alle tidspunkter (24 timer)
"**Fra**" – "**til**" Hændelsen er begrænset tidsligt.

13.2 Serverkonfigurering

Der kan gemmes 5 servere i netværkkameraet. Klik på **"Tilføj"** for at konfigurere en ny server. Serveren af typen **"SD"** er forindstillet og betegner SD-kort-enheden som mål for datalagringerne. Følgende servertyper kan konfigureres:

- E-mail: Indtast adgangsdataene her
- FTP: Indtast adgangsdataene her. Adressekonvention: ftp.abus-sc.com
- HTTP: Indtast adgangsdataene her. Adressekonvention: http://abus-sc.com/cgi-bin/upload.cgi
- Netdrev: Adressekonvention: \\192.160.0.5\NAS

Servernavn:
Servertype
E-mail:
Afsender-e-mailadresse:
Modtager e-mailadresse:
Serveradresse:
Brugernavn:
Password:
Serverport 25
Serveren kræver en sikker forbindelse (SSL)
FTP:
HTTP:
Netdrev:
Test Gem Luk

Når adgangsdataene er indtastet, skal indstillingerne gemmes. Før du lukker vinduet, anbefales det at gennemføre en **"test"**. Resultatet vises i et nyt vindue i browseren.

13.3 Medieindstillinger

Der kan gemmes 5 medieindstillinger i videoserveren.

Medienavn:

Medietype

(•) Momentoptagelse

Kilde: Stream1

Send 1 Foralarmbilled(er) [0~7]

Send 1 Efteralarmbilled(er) [0~7]

Filnavn-tilføjelse:

☐ Vedhæft dato og klokkeslæt til filnavnet

( ) Video klip

( ) Log-fi

( ) Custom Message

Gem Luk

"Medienavn" Entydigt navn for mediet.

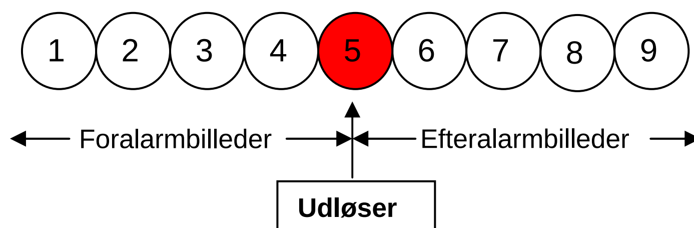
Der findes 4 forskellige medietyper:

- Momentoptagelse (filformat JPEG)
- Videoklip (filformat MP4)
- Log-fil (filformat TXT)
- Custom Message (filformat TXT)

Hvert oprettet medium må kun sammenknyttes med en hændelse.
En dobbelt belægning af et medium medfører, at videoserveren arbejder ukorrekt.
Hvis du ønsker at anvende den samme medietype til to hændelser, skal der forinden også være oprettet to separate medietyper.

Momentoptagelse

"Kilde" Optagelsen kan foretages af videostream 1-4
"Send foralarmbilleder" Antal momentoptagelser før en hændelse
"Send efteralarmbilleder" Antal momentoptagelser efter en hændelse



"Filnavn-tilføjelse" Indtast her en betegnelse, der stilles foran filnavnet ved momentoptagelsen.
"Vedhæft dato og klokkeslæt til filnavnet" Med denne option forsyner den optagede momentoptagelse med dato og klokkeslæt for let at kunne skelne momentoptagelsernes filnavne fra hinanden enten i sekventiel eller hændelsesstyret drift. F.eks. betyder "video@20030102_030405.jpg", at JPEG-billedet blev optaget den 2. januar 2003, kl. 3, 4 minutter og 5 sekunder. Hvis dette suffix udelades, opdateres filen med betegnelsen "video.jpg" på den eksterne FTP-server efter det indstillede tidsinterval.

Filnavnet er opbygget på følgende måde:
Tilføjelse_YYYYMMDD_HHMMSS : ABUS_20091115_164501

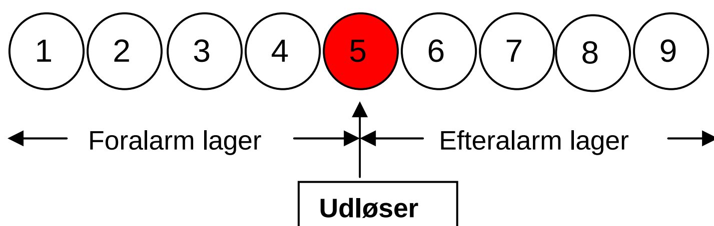
- Tilføjelse: Se Filnavn-tilføjelse
- Y: Joker for år, YYYY = 2009
- M: Joker for måned, MM = 11
- D: Joker for dag, DD = 15
- H: Joker for time, HH = 16
- M: Joker for minut, MM = 45
- S: Joker for sekund, SS = 01

Videoklip

“Kilde” Optagelsen kan foretages af videostream 1 – 4.

Videostream’en, der er konfigureret under “Audio og video” for “Videobuffer”, tilbydes som kilde.

“Foralarm-optagelse” Foralarm-optagelsesinterval i sekunder (maks. 9 sekunder)
“Maksimal varighed” Maksimal varighed pr. fil (maks. 10 sekunder)



“Maksimal filstørrelse” Filens maksimale størrelse i kByte (maks. 800 kByte)
“Filnavn-tilføjelse” Indtast her en betegnelse, der stilles foran filnavnet ved videooptagelsen (detaljer, se Momentoptagelse)

Log-fil
Gemmer det aktuelle system-log-indhold i en tekstfil.

Custom Message
En brugerdefineret melding i form af en tekstfil sendes med.

13.4 Handling

Handling

Digital udgang aktiv for 1 Sekunder

Back-up media wanneer de verbinding met het netwerk verbroken is

Gå til preset position

Oplysning: Konfigurering Forudindstillede steder først

Tilføj server | Tilføj medie

	Server	Medie	
☐	SD	-----None-----	SD Test · Se
☑	NAS	Snapshot	☐ Opret mapper automatisk
			Tilpassede mappe %IP/%Y%M%D/%H_MeinBeispieltext
			Se

Gem | Luk

Konfigurer her handlingen, som skal udføres, når der foreligger en udløst alarm.

“Digital udgang aktiv for” Ved aktivering kobles videoserverens relæudgang.
“Gå til preset position” Der aktiveres en preset-position ved alarm
“Server” Det valgte medium sendes til en bestemte server (f.eks.: En e-mail sendes med en momentoptagelse).

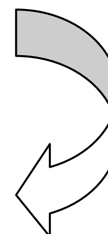
“Opret mapper automatisk” Opretter automatisk mapper i netværksdrevets bibliotek
“Tilpasset mappe” Ved hjælp af variabler fastlægges mappens specifikke betegnelse.
Find variablerne, der står til rådighed i nedenstående tabel.

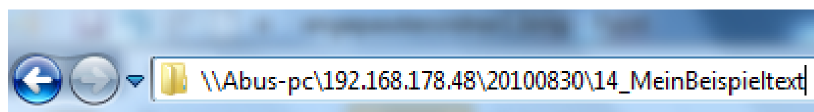
Symbol	Eksempel/funktion
/	*Opret ny undermappe*
%IP = IP-adresse	*192.168.0.1*
%N = hændelsesnavn	*Motion_W1*
%Y = år	*2010*
%M = måned	*03*
%D = dag	*04*
%H = time	*14*
“_Eksempeltekst”	*“_Eksempeltekst”*

Eksempel:
Følgende indtastning opretter denne sti.

☐ Opret mapper automatisk

Tilpassede mappe : %IP/%Y%M%D/%H_MeinBeispieltext





13.5 Anvendelsesoversigt

Her vises alle “Hændelser”, “Medietyper” og “Server”, der er indstillet i videoserveren.
Her kan du kontrollere og slette de forskellige indstillinger og tilføje nye.
Derudover kan forskellige parametre som f.eks.
navn, status, udløser, sted og adresse kontrolleres.

Hændelsessetup

Navn	Status	Søn	Man	Tir	Med	Tor	Fre	Lør	Tid	Udløser
ABUS	ON	V	V	V	V	V	V	V	00:00~24:00	boot

Tilføj | ABUS | Slet | Hjælp

Serverindstillinger

Navn	Type	Adresse/Sted
NAS	ns	\\my_nas\disk\folder

Tilføj | Slet

Medium

Ledig hukommelse: 9550KB

Navn	Type
Snapshot	snapshot

Tilføj | Slet

14. Optagelse

Området Optagelse anvendes til at indstille optagelser med den forskel, at der her kan indstilles permanente videooptagelser for SD-kort eller netværksfrigivelser. Der kan gemmes to optagelsesindstillinger i videoserveren. Opret en ny optagelse ved at klikke på **"Tilføj"**

Optagelsesnavn: Video
Aktiver optagelse
Prioritet: Normal
Kilde: Stream1
Udløser
Kalender
Network fail
Optagelseskalender
Søn Man Tir Med Tor Fre Lør
Tid
Altid
Fra 00:00 til 24:00 [hh:mm]
Mål SD
Vigtig: For at aktivere optagelse, venligst To enable recording notification please configure Anvendelse

Mål: **"Netværksdrev"**

Mål NAS
Kapacitet:
Hele det ubenyttede plads
Reserveret plads: 15 Mbytes
Filnavn-tilføjelse:
Opret mapper automatisk
Tilpassede mappe : %Y%M%D/%H
Aktiver cyklisk optagelse
Vigtig: For at aktivere optagelse, venligst To enable recording notification please configure
Anvendelse først
Gem Luk

"Optagelsesnavn" Et entydigt navn for en optagelsespost.
"Aktiver optagelse" Sæt flueben for at aktivere optagelsespost.
"Prioritrt" Optagelsen med højere prioritet udføres først.
"Kilde" Optagelsen kan foretages af videostream 1 – 4.
"Tidsplan" Optagelsestidsplanen anvendes
"Netværksfejl" Hvis der forekommer en netværksfejl, aktiveres der automatisk en backup på SD-kortet
"Søn" – **"Lør"** vælger ugedagene for udførelsen af optagelsen.
"Altid" Aktiverer optagelsen på alle tidspunkter.
"Fra" – **"til"** Optagelsen er begrænset tidsligt.
"Mål" SD-kort eller netværksmappe
"Samlet lagerplads" Lagerpladsen, der maksimalt står til rådighed på mållageret, anvendes.
"Reserveret plads" Angiver, hvor mange MB fri lagerplads der forreserveres.

Gå til kapitel “13.4 Handling” for mere præcise henvisninger til “Opret mappe automatisk”.
Når funktionen “Tilpasset mappe” er aktiveret, kan ringlagerfunktionen ikke anvendes.

“Aktiver ringlager” Tilkobler ringlagerfunktionen. Hvis den indstillede værdi nås ved backup, overskrives de ældste data.

Optagelsesoversigt

“Navn (video)” Åbner optagelseskonfigureringssiden
“Status (ON)” Indstiller optagelsens status på TIL/FRA
“Mål (SD)” Åbner en filliste med de gemte optagelser

Optagelsesindstillinger

Navn	Status	Søn	Man	Tir	Med	Tor	Fre	Lør	Tid	Kilde	Mål
ABUS	ON	V	V	V	V	V	V	V	00:00~24:00	stream1	SD

Tilføj | SD Test | ABUS | Slet

15. Lokalt lager

Dette afsnit forklarer, hvordan videoserverens lokale lager (SD-kort) kan forvaltes. Kort af typen SD/SDHC Class 6 på indtil 32 GByte understøttes.

Forvaltning af SD-kortet

SD kort indstillinger

SD kort status: Klar

Total størrelse: 3860600 KBytes — tom plads: 3580608 KBytes

Brugt størrelseUsed size:279992 KBytes — Anvend (%): 7.253 %

Format

SD kort kontrol:

Aktiver cyklisk lagring

Aktiver automatisk disk oprydning

Maximum duration for keeping files: 7 Dage

Gem

Anvend funktionen **“Format”**, når du anvender kortet første gang i videoserveren

Hvis optionen **“Aktiver cyklisk lagring”** aktiveres, overskrives de ældste data først, når SD-kortets lagerkapacitet er nået.

Hvis optionen **“Automatisk disk oprydning”** aktiveres, slettes SD-kortet komplet efter indtastning af den maksimale forvirkningstid.

Søgning efter og visning af optagelserne
Hvis der ikke vælges et kriterium, vises alle optagelser altid i resultatlisten

Søge og afspille optagelser

Fil egenskaber:

Udløsertype:	☐ Digital indput	☐ Tabt videosignal	☐ Video restore
	☐ Systemgenstart	☐ Optagelses besked	☐ Bevægelse
	☐ Periodisk	☐ Netværksfejl	☐ IP ændret
	☐ Sabotage		
Medietype:	☐ Video klip	☐ Momentoptagelse	☐ Tekst
Låst:	☐ Låst	☐ Åbnet	

Trigger tid:

Fra:	Dato		Tid	
til:	Dato		Tid	
		(yyyy-mm-dd)		(hh:mm:ss)

Søg

"Udløsertype" Vælg et eller flere kriterier, som en optagelse på SD-kortet ved hjælp af.
"Trigger tid" Vælg det ønskede tidsrum

Klik på "Søg". Alle de optagelser, der opfylder kriterierne, vises i resultatlisten.

Resultatliste

Antal elementer på en side

Søge resultater

Show 10 entries — Search: — Søgnin

	Trigger tid	Medietype	Udløsertype	Låst
☐	2010-01-02 10:44:13	Video klip	Periodisk	Nej
☐	2010-01-02 10:45:13	Video klip	Periodisk	Nej
☐	2010-01-02 10:46:13	Video klip	Periodisk	Nej
☐	2010-01-02 10:47:13	Video klip	Periodisk	Nej
☐	2010-01-02 10:48:13	Video klip	Periodisk	Nej
☐	2010-01-02 10:49:12	Video klip	Periodisk	Nej
☐	2010-01-02 10:50:12	Video klip	Periodisk	Nej
☐	2010-01-02 10:51:11	Video klip	Periodisk	Nej
☐	2010-01-02 10:52:11	Video klip	Periodisk	Nej
☐	2010-01-02 10:53:10	Video klip	Periodisk	Nej

Showing 1 to 10 of 11 entries — Bladring af sider

Se | Download | Fjern markeringen fra alt | JPEGs til AVI | Lås/Åbne | Fjern

"Se" Viser den valgte optagelse i et nyt vindue.
"Download" Tilbyder at downloade den valgte optagelse.
"JPEG til AVI" Flere JPEG-enkeltbilledeoptagelser kan vælges (valgfelt) og konverteres til en AVI-fil.

“Lås/Åbne” Enkelte optagelser blokeres. Blokerede optagelser overskrives ikke under den cykliske lagring. Frigivelser fjerner denne attribut igen.
“Fjern” Den valgte optagelse slettes

Som alternativ kan du også analysere dataene, der er gemt på SD-kortet, med SD-kortlæseren på dit pc-system. De optagede data vises i henhold til deres filendelse med dato og klokkeslæt i filnavnet.

16. Log-fil

Klik på dette link på konfigureringssiden for at vise systemprotokolfilen. Filens indhold giver ekstra informationer om konfigureringen og forbindelsen, når systemet er startet. Log-filens standard er RFC 3164. Du kan evt. sende dataene til en log-server. Aktiver optionen “Remote-protokol”, og indtast serverens IP-adresse og portnummer.

17. Parameterliste

Klik på dette link på konfigureringssiden for at vise alle systemets parameterposter. Disse informationer kan stilles til rådighed i forbindelse med support.

18. Forvaltning

Genstart

Genstartindstillinger

Vigtigt: Når du vælger sekvens genstarter apparatet kl. 24:00 hver x dag [x].

Genstart

Sekvens :

Alle 1 [1~30] Dag[e]

Tidsplan :

Søn Man Tir Med Tor Fre Lør

Tid 00:00 [hh:mm]

Gem Genstart nu

Gem | Genstart nu

Gendan

Nulstil alle indstillinger til fabriksindstillinger bortset fra

☐ Netværkstype ☐ Sommertid

Gendan

Eksporter filer

Eksporter sommertid konfigureringsfile — Eksport

Eksporter indstillinger til backup fil — Eksport

Upload filer

Opdater sommertid-indstillinger — Durchsuchen... — Upload

Upload indstillinger af backup filen — Durchsuchen... — Upload

Firmware-opdatering

Vælg firmware-fil — Durchsuchen...

Opdatering

Genstart af system
Tryk på kontaktfladen “Genstart nu” for at genstarte videoserveren. Som alternativ kan du konfigurere en automatiseret genstart af apparatet. Det kan være nyttigt ved netværksproblemer. Ved problemer anbefaler vi at genstarte videoserveren en gang om ugen.

Gendannelse
Tryk på kontaktfladen for at gendanne forindstillingerne fra fabrikken. Alle indstillinger, der hidtil er foretaget, mistes dermed.

Eksport af fil
Tryk på kontaktfladen for at eksportere din videoserverindstilling til en fil. Konfigureringsfilen for sommertid kan også eksporteres og sikres.

Upload af fil
Tryk på “Durchsuchen…”, og vælg den passende konfigureringsfil.
Tryk derefter på “Upload”, og vent, indtil indstillingerne er blevet gendannet.

Opdatering af firmware
Analogt med opdatering med installationsassistenten er det her muligt at bringe videoserverens firmware på den nyeste stand. Den mest aktuelle firmware kan fås under www.abus-sc.com. Vælg opdateringsfilen (*.pkg), og tryk på kontaktfladen Opdatering. Opdateringen tager lidt tid. Når videoserveren derefter er genstartet, tages den i drift med den nye firmware.

Afbryd under ingen omstændigheder videoserveren fra strømmen under en firmware-opdatering. Der er fare for en irreparabel beskadigelse.
En firmware-opdatering kan være indtil 10 minutter.

19. Vedligeholdelse og rengøring

19.1 Funktionstest

Kontrollér regelmæssigt produktets tekniske sikkerhed, f.eks. beskadigelse af huset..

Hvis det antages, at drift ikke længere er mulig uden farer, skal produktet tages ud af drift og sikres mod utilsigtet drift.

Det antages, at drift ikke længere er mulig uden farer, hvis

- apparatet har synlige beskadigelser,
- apparatet ikke længere fungerer,
- apparatet har været opbevaret i længere tid under ugunstige forhold,
- apparatet har være udsat for alvorlige transportbelastninger.

Produktet er for dig vedligeholdelsesfrit. Der er ingen bestanddele inde i produktet, som du skal kontrollere eller vedligeholde, åbn det aldrig.

19.2 Rengøring

Rengør produktet med en ren, tør klud. Ved kraftigere tilsmudsninger kan kluden fugtes let med lunkent vand.

Sørg for, at der ikke kommer væsker ind i apparatets indre. Derved ødelægges apparatet. Anvend ikke kemiske rengøringsmidler. Derved kan husets overflade blive angrebet.

20. Bortskaffelse

Apparater med dette mærke må ikke bortskaffes sammen med husholdningsaffaldet. Bortskaf produktet iht. de gældende lovmæssige bestemmelser, når dets levetid er afsluttet.
Kontakt din forhandler eller bortskaf produkterne hos den kommunale genbrugsstation for elskrot.

21. Tekniske data

Typenummer	TVIP40000
Kameratype	Videoserver
Opløsning	QCIF,CIF,4CIF,D1 176x144 - 720x576 (mellemtrin kan vælges frit)
Billedelementer (total)	720x576
Billedelementer (effektive)	720x576
Digitalt zoom	4 x
Billedkomprimering	H.264, MPEG-4, MJPEG
Billedhastighed	H.264 720X480@30FPS, 720x576@25FPS
	MPEG-4 720X480@30FPS, 720x576@25FPS
	MJPEG 720X480@30FPS, 720x576@25FPS
Videostandard	PAL, NTSC
Antal parallelle streams	4
Maksimalt antal brugere	10
Bevægelsesgenkendelse	3 zoner
For-/efteralarmlager	Ja
Billed-overlay	Dato, kameranavn, privatzoner
Alarmindgang (NO/NC)	1
Digital udgang	1 (12VDC@400mA)
Audio	Audioudgang (speaker out), audioindgang, 2-vejs-audio
Alarmmelding	E-mail / FTP / HTTP-meddelelse / relæudgang / NAS-drev / SD-kort
Understøttede browsere	Mozilla Firefox eller Internet Explorer 6.x eller højere
Understøttet software	eytron VMS, ONVIF understøttelse
SD-kort	Maks. 32 GB (SD/SD-HC)
RS-485-tilslutning	Ja
PTZ-protokoller	Pelco D, Pelco P, LiLin, Samsung scc643, DynaDome / SmartDome
Netværkstilslutning	RJ-45 ethernet 10/100 Base-T med PoE
Netværksprotokol	IPv4, IPv6, TCP/IP, HTTP, UPnP, RTSP/RTP/RTCP, IGMP, SMTP, FTP, DHCP, NTP, DNS, CoS, QoS, SNMP, 802.1X
Aflåsning	HTTPS SSLv3
Adgangsbeskyttelse	IP-adressefilter, brugernavn, kodeord, 3 adgangstrin
Spændingsforsyning	12 V DC, 24 V AC, 802.3af PoE
Strømforbrug	Maks. 5,0 watt
Driftstemperatur	0 °C ~ 55 °C
Mål (BxHxD)	75 x 35 x 150 mm
Certificeringer	CE, RoHS, C-Tick

22. URL-kommandoer

For kunder, som allerede har en egen hjemmeside eller web-styringsanvendelse, kan netværksvideoserver nemt integreres via URL'er. I dette afsnit er kommandoerne opført i netværksvideoservers URL-format. Forklaringerne findes på engelsk i vejledningens appendiks.

23. GPL-licensoplysninger

Vi gør også her opmærksom på, at netværkvideoserver TVIP40000 bl.a. indeholder Linux-softwareprogrammer, som udelukkende bliver licenseret i GNU General Public License (GPL). For at sikre en GPL-konform anvendelse af programmerne henviser vi til GPL's licensbetingelser.

Licenstekst

Licensteksten til GNU General Public Licence kan også ses på den vedlagte software-CD eller på ABUS Security-Centers hjemmeside på
http://www.abus-sc.de/DE/Service-Downloads/Software?q=GPL
.

Kildekode

De anvendte kildekoder står på ABUS Security-Centers hjemmeside på
http://www.abus-sc.de/DE/Service-Downloads/Software?q=GPL
parat som gratis download.

Udførligheden af hele systemet

De softwarepakker (Source Codes), som tilbydes som download, gør det ikke muligt at oprette et fungerende komplet system. Dertil mangler forskellige softwareprogrammer og den hardware, der er blevet udviklet for netværkskamerasystemet.

24. Teknologi-licensoplysninger

Technologie H.264, MPEG-4 AAC

CE PRODUIT EST CONCÉDÉ SELON LES CONDITIONS DE LA LICENCE DE BREVET H.264, MPEG-4 AAC AUDIO. IL NE DOIT FAIRE L'OBJET D'AUCUNE DÉCOMPILATION, INGÉNIERIE INVERSE OU COPIE, À L'EXCEPTION DE LA COPIE UNIQUE AUTORISÉE À DES FINS D'ARCHIVAGE POUR LES LOGICIELS INFORMATIQUES. POUR PLUS D'INFORMATIONS, VEUILLEZ CONSULTER LE SITE HTTP://WWW.VIALICENSING.COM.

Technologie H.264, MPEG-4 Visual

CE PRODUIT EST CONCÉDÉ SELON LES CONDITIONS DE LA LICENCE DE PORTEFEUILLE DE BREVETS H.264, MPEG-4 VISUAL DANS LE CADRE DE L'UTILISATION PERSONNELLE ET NON COMMERCIALE D'UN CONSOMMATEUR EN VUE (i) DE L'ENCODAGE VIDÉO CONFORMÉMENT À LA NORME MPEG-4 VISUAL (« MPEG-4 VIDEO ») ET/OU (ii) DU DÉCODAGE DE CONTENU H.264, MPEG-4 VIDEO QUI A ÉTÉ ENCODÉ PAR UN CONSOMMATEUR ENGAGÉ DANS UNE ACTIVITÉ PERSONNELLE ET NON COMMERCIALE ET/OU A ÉTÉ OBTENU AUPRÈS D'UN FOURNISSEUR VIDÉO AUTORISÉ PAR MPEG LA À FOURNIR DU CONTENU MPEG-4 VIDEO. AUCUNE LICENCE N'EST ACCORDÉE DE MANIÈRE EXPLICITE OU IMPLICITE POUR AUCUN AUTRE USAGE. POUR DE PLUS AMPLES INFORMATIONS, Y COMPRIS AU SUJET DES UTILISATIONS ET DES LICENCES PROMOTIONNELLES, INTERNES ET COMMERCIALES, VEUILLEZ VOUS ADRESSER À MPEG LA, LLC. VOIR
20. HTTP://WWW.MPEGLA.COM.

Norme AMR-NB

CE PRODUIT EST CONCÉDÉ SELON LES CONDITIONS DE LA LICENCE DE BREVET DE LA NORME AMR-NB. L'UTILISATION DE CE PRODUIT PEUT ÊTRE SOUMISE À L'APPLICATION DES BREVETS DES CONCÉDANTS DE LICENCE SUIVANTS :

TELEFONAKIEBOLAGET ERICSSON AB : US PAT. 6192335; 6275798; 6029125; 6424938; 6058359. NOKIA CORPORATION : US PAT. 5946651; 6199035. VOICEAGE CORPORATION : AT PAT. 0516621; BE PAT. 0516621; CA PAT. 2010830; CH PAT. 0516621; DE PAT. 0516621; DK PAT. 0516621; ES PAT. 0516621; FR PAT. 0516621; GB PAT. 0516621; GR PAT. 0516621; IT PAT. 0516621; LI PAT. 0516621; LU PAT. 0516621; NL PAT. 0516621; SE PAT 0516621; US PAT 5444816; AT PAT. 819303/AT E 198805T1; AU PAT. 697256; BE PAT. 819303; BR PAT. 9604838-7; CA PAT. 2216315; CH PAT. 819303; CN PAT. ZL96193827.7; DE PAT. 819303/DE69611607T2; DK PAT. 819303; ES PAT. 819303; EP PAT. 819303; FR PAT. 819303; GB PAT. 819303; IT PAT. 819303; JP PAT. APP. 8-529817; NL PAT. 819303; SE PAT. 819303; US PAT. 5664053. CETTE LISTE PEUT ÊTRE MISE À JOUR À TOUT MOMENT PAR LES CONCÉDANTS DE LICENCE. LA VERSION LA PLUS RÉCENTE DE CETTE LISTE EST DISPONIBLE SUR LE SITE WEB DES CONCÉDANTS DE LICENCE À L'ADRESSE HTTP://WWW.VOICEAGE.COM.

Appendix

A.) Bandwidth and memory usage

MPEG-4

QCIF

Fixed Quality	Medium	Standard	Good	Detailed	Excellent
Frame Size (KBytes)	0,49	0,59	1,15	1,35	1,74
Frames per Second	30	30	30	30	30
Record Size per Second (MBytes)	0,0147	0,0177	0,0345	0,0405	0,0522
Record Size per Minute (MBytes)	0,882	1,062	2,07	2,43	3,132
Record Size per Hour (MBytes)	52,92	63,72	124,2	145,8	187,92
Record Size per Day (MBytes)	1270,08	1529,28	2980,8	3499,2	4510,08

CIF

Fixed Quality	Medium	Standard	Good	Detailed	Excellent
Frame Size (KBytes)	1,3	1,67	2,58	3,9	5,4
Frames per Second	30	30	30	30	30
Record Size per Second (MBytes)	0,039	0,0501	0,0774	0,117	0,162
Record Size per Minute (MBytes)	2,34	3,006	4,644	7,02	9,72
Record Size per Hour (MBytes)	140,4	180,36	278,64	421,2	583,2
Record Size per Day (MBytes)	3369,6	4328,64	6687,36	10108,8	13996,8

4CIF

Fixed Quality	Medium	Standard	Good	Detailed	Excellent
Frame Size (KBytes)	3,45	5,4	7,65	10,1	13,8
Frames per Second	30	30	30	30	30
Record Size per Second (MBytes)	0,1035	0,162	0,2295	0,303	0,414
Record Size per Minute (MBytes)	6,21	9,72	13,77	18,18	24,84
Record Size per Hour (MBytes)	372,6	583,2	826,2	1090,8	1490,4
Record Size per Day (MBytes)	8942,4	13996,8	19828,8	26179,2	35769,6

D1

Fixed Quality	Medium	Standard	Good	Detailed	Excellent
Frame Size (KBytes)	3,6	6,2	7,3	10,7	14,5
Frames per Second	30	30	30	30	30
Record Size per Second (MBytes)	0,108	0,186	0,219	0,321	0,435
Record Size per Minute (MBytes)	6,48	11,16	13,14	19,26	26,1
Record Size per Hour (MBytes)	388,8	669,6	788,4	1155,6	1566
Record Size per Day (MBytes)	9331,2	16070,4	18921,6	27734,4	37584

Motion JPEG

QCIF

Fixed Quality	Medium	Standard	Good	Detailed	Excellent
Frame Size (KBytes)	3,3	4,2	5,15	6,52	10,6
Frames per Second	30	30	30	30	30
Record Size per Second (MBytes)	0,099	0,126	0,1545	0,1956	0,318
Record Size per Minute (MBytes)	5,94	7,56	9,27	11,736	19,08
Record Size per Hour (MBytes)	356,4	453,6	556,2	704,16	1144,8
Record Size per Day (MBytes)	8553,6	10886,4	13348,8	16899,84	27475,2

CIF

Fixed Quality	Medium	Standard	Good	Detailed	Excellent
Frame Size (KBytes)	7,6	9,8	12,15	15,8	26,8
Frames per Second	30	30	30	30	30
Record Size per Second (MBytes)	0,228	0,294	0,3645	0,474	0,804
Record Size per Minute (MBytes)	13,68	17,64	21,87	28,44	48,24
Record Size per Hour (MBytes)	820,8	1058,4	1312,2	1706,4	2894,4
Record Size per Day (MBytes)	19699,2	25401,6	31492,8	40953,6	69465,6

4CIF

Fixed Quality	Medium	Standard	Good	Detailed	Excellent
Frame Size (KBytes)	20,2	26,3	31,8	39,8	71,7
Frames per Second	30	30	30	30	30
Record Size per Second (MBytes)	0,606	0,789	0,954	1,194	2,151
Record Size per Minute (MBytes)	36,36	47,34	57,24	71,64	129,06
Record Size per Hour (MBytes)	2181,6	2840,4	3434,4	4298,4	7743,6
Record Size per Day (MBytes)	52358,4	68169,6	82425,6	103161,6	185846,4

D1

Fixed Quality	Medium	Standard	Good	Detailed	Excellent
Frame Size (KBytes)	21	26,6	35,5	40,7	72,2
Frames per Second	30	30	30	30	30
Record Size per Second (MBytes)	0,63	0,798	1,065	1,221	2,166
Record Size per Minute (MBytes)	37,8	47,88	63,9	73,26	129,96
Record Size per Hour (MBytes)	2268	2872,8	3834	4395,6	7797,6
Record Size per Day (MBytes)	54432	68947,2	92016	105494,4	187142,4

H.264

QCIF	Medium				
Fixed Quality	0,38	Standard	Good	Detailed	Excellent
Frame Size (KBytes)	30	0,48	0,98	1,28	1,65
Frames per Second	0,0114	30	30	30	30
Record Size per Second (MBytes)	0,684	0,0144	0,0294	0,0384	0,0495
Record Size per Minute (MBytes)	41,04	0,864	1,764	2,304	2,97
Record Size per Hour (MBytes)	984,96	51,84	105,84	138,24	178,2
Record Size per Day (MBytes)		1244,16	2540,16	3317,76	4276,8

CIF	Medium				
Fixed Quality	0,79	Standard	Good	Detailed	Excellent
Frame Size (KBytes)	30	1,12	1,48	2,76	3,93
Frames per Second	0,0237	30	30	30	30
Record Size per Second (MBytes)	1,422	0,0336	0,0444	0,0828	0,1179
Record Size per Minute (MBytes)	85,32	2,016	2,664	4,968	7,074
Record Size per Hour (MBytes)	2047,68	120,96	159,84	298,08	424,44
Record Size per Day (MBytes)		2903,04	3836,16	7153,92	10186,56

4CIF	Medium				
Fixed Quality	1,89	Standard	Good	Detailed	Excellent
Frame Size (KBytes)	30	2,2	4,6	7,13	12,6
Frames per Second	0,0567	30	30	30	30
Record Size per Second (MBytes)	3,402	0,066	0,138	0,2139	0,378
Record Size per Minute (MBytes)	204,12	3,96	8,28	12,834	22,68
Record Size per Hour (MBytes)	4898,88	237,6	496,8	770,04	1360,8
Record Size per Day (MBytes)		5702,4	11923,2	18480,96	32659,2

D1	Medium				
Fixed Quality	2,1	Standard	Good	Detailed	Excellent
Frame Size (KBytes)	30	2,6	5,3	8,5	13,3
Frames per Second	0,063	30	30	30	30
Record Size per Second (MBytes)	3,78	0,078	0,159	0,255	0,399
Record Size per Minute (MBytes)	226,8	4,68	9,54	15,3	23,94
Record Size per Hour (MBytes)	5443,2	280,8	572,4	918	1436,4
Record Size per Day (MBytes)		6739,2	13737,6	22032	34473,6

B.) HTTP/CGI Command

In URL syntax and in descriptions of CGI parameters, a text within angle brackets denotes a content that is to be replaced with either a value or a string. When replacing the text string also the angle brackets shall be replaced. An example of this is the description of the name for the server, denoted with <servername> in the URL syntax description below, that is replaced with the string myserver in the URL syntax example, also below.

URL syntax' are written with the “**Syntax:**" word written in bold face followed by a box with the referred syntax as seen below. The name of the server is written as <servername>. This is intended to be replaced with the name of the actual server. This can either be a name, e.g., "mywebcam" or "thecam.adomain.net" or the associated IP number for the server, e.g., 192.168.0.220.

Special note will be marked as RED words to take care.

General CGI URL syntax and parameters

CGI parameters are written in lower-case and as one word without any underscores or other separators. When the CGI request includes internal camera parameters, the internal parameters must be written exactly as they are named in the camera or video server. The CGIs are organized in function related directories under the cgi-bin directory. The file extension of the CGI is required.

Syntax:

```
http://<servername>/cgi-bin/<subdir>[/<subdir>...]/<cgi>.<ext>
[?<parameter>=<value>[&<parameter>=<value>...]]
```

Example: Setting digital output #1 to active

http://mywebserver/cgi-bin/dido/setdo.cgi?do1=1

Security level

SECURITY LEVEL	SUB-DIRECTORY	DESCRIPTION
0	anonymous	Unprotected.
1 [view]	anonymous, viewer, dido, camctrl	1. Can view, listen, talk to camera 2. Can control dido, ptz of camera
4 [operator]	anonymous, viewer, dido, camctrl, operator	Operator’s access right can modify most of camera’s parameters except some privilege and network options
6 [admin]	anonymous, viewer, dido, camctrl, operator, admin	Administrator’s access right can fully control the camera’s operation.
7	N/A	Internal parameters. Unable to be changed by any external interface.

Get server parameter values

Note: The access right depends on the URL directory.

Method: GET/POST

Syntax:

http://<*servername*>/cgi-bin/anonymous/getparam.cgi?[<*parameter*>]

[&<parameter>…]

```
http://<servername>/cgi-bin/viewer/getparam.cgi?[<parameter>]
[&<parameter>…]

http://<servername>/cgi-bin/operator/getparam.cgi?[<parameter>]
[&<parameter>…]

http://<servername>/cgi-bin/admin/getparam.cgi?[<parameter>]
[&<parameter>…]
```

where the *<parameter>* should be *<group>*[_*<name>*] or *<group>*[.*<name>*] If you do not specify the any parameters, all the parameters on the server will be returned. If you specify only *<group>*, the parameters of related group will be returned.

When query parameter values, the current parameter value are returned. Successful control request returns paramter pairs as follows.

Return:

```
HTTP/1.0 200 OK\r\n Content-
Type: text/html\r\n Context-Length:
<length>\r\n
\r\n
<parameter pair>
```

where <parameter pair> is

<parameter>=<value>\r\n

[<parameter pair>]

<length> is the actual length of content.

Example: request IP address and it's response

```
Request:
http://192.168.0.123/cgi-bin/admin/getparam.cgi?network_ipaddress

Response:
HTTP/1.0 200 OK\r\n Content-
Type: text/html\r\n Context-
Length: 33\r\n
\r\n network.ipaddress=192.168.0.123\r\n
```

Set server parameter values

Note: The access right depends on the URL directory.

Method: GET/POST

Syntax:

http://<*servername*>/cgi-bin/anonymous/setparam.cgi? <*parameter*>=<*value*>
[&<parameter>=<value>…][&update=<value>][&return=<return page>]

http://<*servername*>/cgi-bin/viewer/setparam.cgi? <*parameter*>=<*value*>
[&<parameter>=<value>…][&update=<value>] [&return=<return page>]

http://<*servername*>/cgi-bin/operator/setparam.cgi? <*parameter*>=<*value*>
[&<parameter>=<value>…][&update=<value>] [&return=<return page>]

http://<*servername*>/cgi-bin/admin/setparam.cgi? <*parameter*>=<*value*>
[&<parameter>=<value>…][&update=<value>] [&return=<return page>]

PARAMETER	VALUE	DESCRIPTION
<group>_<name>	value to assigned	Assign <*value*> to the parameter <*group*>_<*name*>
update	<boolean>	set to 1 to actually update all fields (no need to use update parameter in each group)
return	<*return page*>	Redirect to the page <*return page*> after the parameter is assigned. The <*return page*> can be a full URL path or relative path according to the current path. If you omit this parameter, it will redirect to an empty page. (note: The return page can be a general HTML file(.htm, .html) or a VIVOTEK server script executable (.vspx) file. It can not be a CGI command. It can not have any extra parameters. This parameter must be put at end of parameter list)

Return:

HTTP/1.0 200 OK\r\n Content-
Type: text/html\r\n Context-Length:
<length>\r\n

\r\n

<parameter pair>

where <parameter pair> is

<parameter>=<value>\r\n

[<parameter pair>]

Only the parameters that you set and readable will be returned.

Example: Set the IP address of server to 192.168.0.123

Request:

http://myserver/cgi-bin/admin/setparam.cgi?network_ipaddress=192.168.0.123

Response:

HTTP/1.0 200 OK\r\n

Content-Type: text/html\r\n

Context-Length: 33\r\n

\r\n network.ipaddress=192.168.0.123\r\n

Available parameters on the server

Valid values:

VALID VALUES	DESCRIPTION
string[<n>]	Text string shorter than 'n' characters. The characters ",', <,>,& are invalid.
password[<n>]	The same as string but display '*' instead
integer	Any number between (-2^{31} – 1) and (2^{31} – 1)
positive integer	Any number between 0 and (2^{32} – 1)
<m> ~ <n>	Any number between 'm' and 'n'
domain name[<n>]	A string limited to contain a domain name shorter than 'n' characters (eg. www.ibm.com)
email address [<n>]	A string limited to contain a email address shorter than 'n' characters (eg. joe@www.ibm.com)
ip address	A string limited to contain an ip address (eg. 192.168.1.1)
mac address	A string limited to contain mac address without hyphen or colon connected
boolean	A boolean value 1 or 0 represents [Yes or No], [True or False], [Enable or Disable].
<value1>, <value2>,	Enumeration. Only given values are valid.

<value3>, …	
blank	A blank string
everything inside <>	As description

NOTE: The camera should prevent to restart when parameter changed. Group:

system

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
hostname	string[40]	1/6	host name of server (Network Camera, Wireless Network Camera, Video Server, Wireless Video Server)
ledoff	<boolean>	6/6	turn on(0) or turn off(1) all led indicators
date	<yyyy/mm/dd>, keep, auto	6/6	Current date of system. Set to ‘keep’ keeping date unchanged. Set to ‘auto’ to use NTP to synchronize date.
time	<hh:mm:ss>, keep, auto	6/6	Current time of system. Set to ‘keep’ keeping time unchanged. Set to ‘auto’ to use NTP to synchronize time.
datetime	<MMDDhhmmYYYY.ss>	6/6	Another current time format of system.
ntp	<domain name>, <ip address>, <blank>	6/6	NTP server *do not use “skip to invoke default server” for default
timezoneindex	-489 ~ 529	6/6	Indicate timezone and area -480: GMT-12:00 Eniwetok, Kwajalein -440: GMT-11:00 Midway Island, Samoa -400: GMT-10:00 Hawaii -360: GMT-09:00 Alaska -320: GMT-08:00 Las Vegas, San_Francisco, Vancouver -280: GMT-07:00 Mountain Time, Denver -281: GMT-07:00 Arizona -240: GMT-06:00 Central America, Central Time, Mexico City, Saskatchewan

			-200: GMT-05:00 Eastern Time, New York, Toronto -201: GMT-05:00 Bogota, Lima, Quito, Indiana -160: GMT-04:00 Atlantic Time, Canada, Caracas, La Paz, Santiago -140: GMT-03:30 Newfoundland -120: GMT-03:00 Brasilia, Buenos Aires, Georgetown, Greenland -80: GMT-02:00 Mid-Atlantic -40: GMT-01:00 Azores, Cape_Verde_IS. 0: GMT Casablanca, Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London 40: GMT 01:00 Amsterdam, Berlin, Rome, Stockholm, Vienna, Madrid, Paris 41: GMT 01:00 Warsaw, Budapest, Bern 80: GMT 02:00 Athens, Helsinki, Istanbul, Riga 81: GMT 02:00 Cairo 82: GMT 02:00 Lebanon, Minsk 83: GMT 02:00 Israel 120: GMT 03:00 Baghdad, Kuwait, Riyadh, Moscow, St. Petersburg, Nairobi 121: GMT 03:00 Iraq 140: GMT 03:30 Tehran 160: GMT 04:00 Abu Dhabi, Muscat, Baku, Tbilisi, Yerevan 180: GMT 04:30 Kabul 200: GMT 05:00 Ekaterinburg, Islamabad, Karachi, Tashkent 220: GMT 05:30 Calcutta, Chennai, Mumbai, New Delhi 230: GMT 05:45 Kathmandu 240: GMT 06:00 Almaty, Novosibirsk, Astana, Dhaka, Sri Jayawardenepura 260: GMT 06:30 Rangoon 280: GMT 07:00 Bangkok, Hanoi, Jakarta, Krasnoyarsk

			320: GMT 08:00 Beijing, Chongging, Hong Kong, Kuala Lumpur, Singapore, Taipei 360: GMT 09:00 Osaka, Sapporo, Tokyo, Seoul, Yakutsk 380: GMT 09:30 Adelaide, Darwin 400: GMT 10:00 Brisbane, Canberra, Melbourne, Sydney, Guam, Vladivostok 440: GMT 11:00 Magadan, Solomon Is., New Caledonia 480: GMT 12:00 Aucklan, Wellington, Fiji, Kamchatka, Marshall Is. 520: GMT 13:00 Nuku'Alofa
daylight_enable	<boolean>	6/6	enable automatic daylight saving to time zone
daylight_dstactualmode	<boolean>	6/7	check if current time is under daylight saving time.
daylight_auto_begintime	string[19]	6/7	display the current daylight saving begin time. (product dependent)
daylight_auto_endtime	string[19]	6/7	display the current daylight saving end time. (product dependent)
updateinterval	0, 3600, 86400, 604800, 2592000	6/6	0 to Disable automatic time adjustment, otherwise, it means the seconds between NTP automatic update interval.
restore	0, <positive integer>	7/6	Restore the system parameters to default value after <value> seconds.
reset	0, <positive integer>	7/6	Restart the server after <value> seconds if <value> is non-negative.
restoreexceptnet	<Any value>	7/6	Restore the system parameters to default value except (ipaddress, subnet, router, dns1, dns2, pppoe). This command can cooperate with other “restoreexceptXYZ” commands. When cooperating with others, the system

			parameters will be restored to default value except a union of combined results.
restoreexceptdst	<Any value>	7/6	Restore the system parameters to default value except all daylight saving time settings. This command can cooperate with other "restoreexceptXYZ" commands. When cooperating with others, the system parameters will be restored to default value except a union of combined results.
restoreexceptlang	<Any Value>	7/6	Restore the system parameters to default value except custom language file user uploaded. This command can cooperate with other "restoreexceptXYZ" commands. When cooperating with others, the system parameters will be restored to default value except a union of combined results.

SubGroup of **system**: **info** (The fields in this group are unchangeable.)

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
modelname	string[40]	0/7	Internal model name of server (eg. IP7139)
extendedmodelname	string[40]	0/7	ODM specific model name of server (eg. DCS-5610). If it is not ODM case, this field will be equal to "modelname"
serialnumber	<mac address>	0/7	12 characters mac address without hyphen connected
firmwareversion	string[40]	0/7	The version of firmware, including model, company, and version number in the format <MODEL-BRAND-VERSION>
language_count	<integer>	0/7	number of webpage language available on the server
language_i<0~(count-1)>	string[16]	0/7	Available language lists
customlanguage_maxcount	<integer>	0/7	Maximum number of custom language supported on the server
customlanguage_count	<integer>	0/7	Number of custom language which has been uploaded to the server

customlanguage_i<0~(max count-1)>	string	0/7	Custom language name

Group: **status**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
di_i<0~(ndi-1)>	<boolean>	1/7	0 => Inactive, normal 1 => Active, triggered
do_i<0~ndi-1)>	<boolean>	1/7	0 => Inactive, normal 1 => Active, triggered
daynight	day, night	7/7	The day/night status judge by light sensor
onlinenum_rtsp	integer	6/7	current RTSP connection numbers
onlinenum_httppush	integer	6/7	current HTTP push server connection numbers
eth_i0	string	1/99	The connection information of ethernet

Group: **di_i<0~(ndi-1)>** (capability.ndi > 0)

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
normalstate	high, low	1/1	indicate whether open circuit or closed circuit represents inactive status

Group: **do_i<0~(ndo-1)>** (capability.ndo > 0)

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
normalstate	open, grounded	1/1	indicate whether open circuit or closed circuit represents inactive status

Group: **security**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
privilege_do	view, operator, admin	6/6	Indicate which privilege and above can control digital output
privilege_camctrl	view, operator, admin	6/6	Indicate which privilege and above can control PTZ
user_i0_name	string[64]	6/7	User's name of root
user_i<1~20>_name	string[64]	6/7	User's name
user_i0_pass	password[64]	6/6	root's password

user_i<1~20>_pass	password[64]	7/6	User's password
user_i0_privilege	viewer, operator, admin	6/7	root's privilege
user_i<1~20>_ privilege	viewer, operator, admin	6/6	User's privilege.

Group: **network**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
type	lan, pppoe	6/6	Network connection type
resetip	<boolean>	6/6	1 => get ipaddress, subnet, router, dns1, dns2 from DHCP server at next reboot 0 => use preset ipaddress, subnet, rounter, dns1, and dns2
ipaddress	<ip address>	6/6	IP address of server
subnet	<ip address>	6/6	subnet mask
router	<ip address>	6/6	default gateway
dns1	<ip address>	6/6	primary DNS server
dns2	<ip address>	6/6	secondary DNS server
wins1	<ip address>	6/6	primary WINS server
wins2	<ip address>	6/6	secondary WINS server

Subgroup of **network: ieee8021x**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	6/6	Enable/disable IEEE 802.1x
eapmethod	eap-peap, eap-tls	6/6	Selected EAP method
identity_peap	String[64]	6/6	PEAP identity
identity_tls	String[64]	6/6	TLS identity
password	String[254]	6/6	Password for TLS
privatekeypassword	String[254]	6/6	Password for PEAP
ca_exist	<boolean>	6/6	CA installed flag
ca_time	<integer>	6/7	CA installed time. Represented in EPOCH
ca_size	<integer>	6/7	CA file size (in bytes)

certificate_exist	<boolean>	6/6	Certificate installed flag (for TLS)
certificate_time	<integer>	6/7	Certificate installed time. Represented in EPOCH
certificate_size	<integer>	6/7	Certificate file size (in bytes)
privatekey_exist	<boolean>	6/6	Private key installed flag (for TLS)
privatekey_time	<integer>	6/7	Private key installed time. Represented in EPOCH
privatekey_size	<integer>	6/7	Private key file size (in bytes)

Subgroup of **network: qos**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
cos_enable	<boolean>	6/6	Enable/disable CoS (IEEE 802.1p)
cos_vlanid	1~4095	6/6	VLAN ID
cos_video	0~7	6/6	Video channel for CoS
cos_audio	0~7	6/6	Audio channel for CoS
cos_eventalarm	0~7	6/6	Event/alarm channel for CoS
cos_management	0~7	6/6	Management channel for CoS
dscp_enable	<boolean>	6/6	Enable/disable DSCP
dscp_video	0~7	6/6	Video channel for DSCP
dscp_audio	0~7	6/6	Audio channel for DSCP
dscp_eventalarm	0~7	6/6	Event/alarm channel for DSCP
dscp_management	0~7	6/6	Management channel for DSCP

Subgroup of **network**: **ipv6**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	6/6	Enable IPv6
addonipaddress	<ip address>	6/6	IPv6 IP address
addonprefixlen	0~128	6/6	IPv6 prefix length
addonrouter	<ip address>	6/6	IPv6 router address
addondns	<ip address>	6/6	IPv6 DNS address
allowoptional	<boolean>	6/6	Allow Manually setup the IP address setting

Subgroup of **network**: **ftp**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
port	21, 1025~65535	6/6	local ftp server port

Subgroup of **network**: **http**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
port	80, 1025 ~ 65535	6/6	HTTP port
alternateport	1025~65535	6/6	Alternative HTTP port
authmode	basic, digest	1/6	HTTP authentication mode
s0_accessname	string[32]	1/6	Http server push access name for stream 1 (capability.protocol.spush_mjpeg =1 and video.stream.count>0)
s1_accessname	string[32]	1/6	Http server push access name for stream 2 (capability.protocol.spush_mjpeg =1 and video.stream.count>1)
s2_accessname	string[32]	1/6	Http server push access name for stream 3 (capability.protocol.spush_mjpeg =1 and video.stream.count>2)
s3_accessname	string[32]	1/6	Http server push access name for stream 4 (capability.protocol.spush_mjpeg =1 and video.stream.count>3)
s4_accessname	string[32]	1/6	Http server push access name for stream 5 (capability.protocol.spush_mjpeg =1 and video.stream.count>4)
anonymousviewing	<boolean>	1/6	Enable anoymous streaming viewing.

Subgroup of **network**: **https**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
port	443, 1025 ~ 65535	6/6	HTTPS port

Subgroup of **network**: **rtsp**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
port	554, 1025 ~ 65535	1/6	RTSP port (capability.protocol.rtsp=1)
anonymousviewing	<boolean>	1/6	Enable anoymous streaming viewing.
authmode	disable, basic, digest	1/6	RTSP authentication mode (capability.protocol.rtsp=1)

s0_accessname	string[3b;42]	1/6	RTSP access name for stream1 (capability.protocol.rtsp=1 and video.stream.count>0)
s1_accessname	string[32]	1/6	RTSP access name for stream2 (capability.protocol.rtsp=1 and video.stream.count>1)
s2_accessname	string[32]	1/6	RTSP access name for stream3 (capability.protocol.rtsp=1 and video.stream.count>2)
s3_accessname	string[32]	1/6	RTSP access name for stream4 (capability.protocol.rtsp=1 and video.stream.count>3)
S4_accessname	string[32]	1/6	RTSP access name for stream5 (capability.protocol.rtsp=1 and video.stream.count>4)
s0_audiotrack	<integer>	6/6	The current audio track for stream1. -1 => audio mute
s1_audiotrack	<integer>	6/6	The current audio track for stream2. -1 => audio mute

Subgroup of **rtsp_s<0~(n-1)>**: **multicast,** n is stream count (capability.protocol.rtp.multicast=1)

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
alwaysmulticast	<boolean>	4/4	Enable always multicast
ipaddress	<ip address>	4/4	Multicast IP address
videoport	1025 ~ 65535	4/4	Multicast video port
audioport	1025 ~ 65535	4/4	Multicast audio port
ttl	1 ~ 255	4/4	Mutlicast time to live value

Subgroup of **network**: **sip**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
port	554, 1025 ~ 65535	6/6	SIP port (capability.protocol.sip=1)

Subgroup of **network**: **rtp**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
videoport	1025 ~ 65535	6/6	video channel port for RTP (capability.protocol.rtp_unicast=1)
audioport	1025 ~ 65535	6/6	audio channel port for RTP (capability.protocol.rtp_unicast=1)

Subgroup of **network**: **pppoe**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
user	string[128]	6/6	PPPoE account user name
pass	password[64]	6/6	PPPoE account password

Group: **ipfilter**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	6/6	Enable or disable ipfilter settings
admin_enable	<boolean>	6/6	Enable or disable the function always allow the admin IP address to access this device
admin_ip	1.0.0.0 ~ 255.255.255.255	6/6	Always allow this IP connect to camera when admin_enable=1
maxconnection	0~10	6/6	Maximum number of concurrent streaming connection(s) limit
allow_i<0~9>_start	1.0.0.0 ~ 255.255.255.255	6/6	Allowed starting IP address for RTSP connection
allow_i<0~9>_end	1.0.0.0 ~ 255.255.255.255	6/6	Allowed ending IP address for RTSP connection
deny_i<0~9>_start	1.0.0.0 ~ 255.255.255.255	6/6	Denied starting IP address for RTSP connection
deny_i<0~9>_end	1.0.0.0 ~ 255.255.255.255	6/6	Denied ending IP address for RTSP connection
ipv6_allow_i<0~9> _start	<ip address>	6/6	Allowed IPv6 starting IP address for RTSP connection
ipv6_allow_i<0~9> _end	<ip address>	6/6	Allowed IPv6 ending IP address for RTSP connection
ipv6_deny_i<0~9>_ start	<ip address>	6/6	Denied IPv6 starting IP address for RTSP connection

ipv6_deny_i<0~9>_end	<ip address>	6/6	Denied IPv6 ending IP address for RTSP connection

Group: **videoin**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
cmosfreq	50, 60	4/4	CMOS frequency (videoin.type=2) (product dependent)
whitebalance	<product dependent>	4/4	auto, auto white balance manual indoor, 3200K fluorescent, 5500K outdoor, > 5500K
atwbvalue1	0 ~ 9999999999	4/4	The auto white balance value.
atwbvalue2	0 ~ 9999999999	4/4	The auto white balance value.
exposurelevel	1 ~ 8	4/4	The target brightness adjust by exposure options 1: darkest 8: brightness
autoiris	<boolean>	4/4	Enable auto Iris (product dependent)
enableblc	<boolean>	4/4	Enable backlight compensation (product dependent)
agc	normal, max	4/4	Set auto gain control to normal level or MAX level (product dependent)

Group: **videoin_c<0~(n-1)>** for n channel products, m is stream number

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
color	0, 1	4/4	0 =>monochrome 1 => color
flip	<boolean>	4/4	flip the image
mirror	<boolean>	4/4	mirror the image
ptzstatus	<integer>	1/7	An 32-bits integer, each bit can be set separately as follows: Bit 0 => Support camera control

			function 0(not support), 1(support) Bit 1 => **Build-in** or **external** camera. 0(external), 1(build-in) Bit 2 => Support **pan** operation. 0(not support), 1(support) Bit 3 => Support **tilt** operation. 0(not support), 1(support) Bit 4 => Support **zoom** operation. 0(not support), 1(support) Bit 5 => Support **focus** operation. 0(not support), 1(support)
text	string[16]	1/4	enclosed caption
imprinttimestamp	<boolean>	4/4	Overlay time stamp on video
maxexposure	1~120	4/4	Maximum exposure time
options	quality, framerate	4/4	To customize video quality first or video frame rate first. (product dependent)
enablepreview	<boolean>	1/4	0: normal mode 1: preview mode (capability_nvideoinprofile > 0)
profile_i<0~(k-1)>_enable	<boolean>	4/4	Enable this profile (capability_nvideoinprofile > 0)
profile_i<0~(k-1)>_policy	day, night, schedule	4/4	When the condition match the policy, use this profile (capability_nvideoinprofile > 0)
profile_i<0~(k-1)>_begintime	hh:mm	4/4	If choose “schedule” mode as profile policy, the begin time of this profile when enabled (capability_nvideoinprofile > 0)
profile_i<0~(k-1)>_endtime	hh:mm	4/4	If choose “schedule” mode as profile policy, the end time of this profile when enabled (capability_nvideoinprofile > 0)
profile_i<0~(k-1)>_maxexposure	1~120	4/4	Maximum exposure time (capability_nvideoinprofile > 0)
profile_i<0~(k-1)>_enableblc	1~8	4/4	Enable backlight compensation
profile_i<0~(k-1)>_exposurelevel	1~8	4/4	The target brightness adjust by exposure options

			1: darkest 8: brightness (capability_nvideoinprofile > 0)
profile_i<0~(k-1)>_agc	0~2	4/4	Set auto gain control to: 0: 2X level 1: 4X level 2: 8X level (capability_nvideoinprofile > 0)
profile_i<0~(k-1)>_autoiris	<boolean>	4/4	Enable auto Iris (capability_nvideoinprofile > 0)
s<0~(m-1)>_codectype	mpeg4, mjpeg	4/4	video codec type
s<0~(m-1)>_resolution	176x144, 320x240, 640x480, 800x600, 1280x960, 1600x1200	4/4	Video resolution in pixel
s<0~(m-1)>_mpeg4_intraper iod	250, 500, 1000, 2000, 3000, 4000	4/4	The period of intra frame in milliseconds
s<0~(m-1)>_mpeg4_ratecon trolmode	cbr, vbr	4/4	cbr, constant bitrate vbr, fix quality
s<0~(m-1)>_mpeg4_quant	1~5, 99	4/4	quality of video when choosing vbr in “ratecontrolmode”. 99 is customized manual input setting. 1 is worst quality and 5 is the best quality.
s<0~(m-1)>_mpeg4_qvalue	1~31	7/4	The specific quality parameter of mpeg4 encoder. 1 is best quality and 31 is the worst quality.
s<0~(m-1)>_mpeg4_bitrate	1000~400000 0	4/4	Set bit rate in bps when choose cbr in “ratecontrolmode”
s<0~(m-1)>_mpeg4_maxfra me	1~15 for quality mode 1~30 for frame rate mode	4/4	set maximum frame rate in fps (for MPEG-4)
s<0~(m-1)>_mjpeg_quant	1 ~ 5, 999	4/4	quality of jpeg video. 999 is customized manual input setting.

			1 is worst quality and 5 is the best quality.
s<0~(m-1)>_mjpeg_qvalue	10~200	7/4	The specific quality parameter of jpeg encoder. 10 is best quality and 200 is the worst quality.
s<0~(m-1)>_mjpeg_maxfra me	1~25, 26~30 (only for NTSC or 60Hz CMOS)	4/4	set maximum frame rate in fps (for JPEG)
s<0~(m-1)>_forcei	1	7/6	Force I frame

Group: **videoinpreview**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
maxexposure	1~120	4/4	Maximum exposure time
exposurelevel	1 ~ 8	4/4	The target brightness adjust by exposure options 1: darkest 8: brightness
enableblc	<boolean>	4/4	Enable backlight compensation (product dependent)
agc	0~2	4/4	Set auto gain control to: 0: 2X level 1: 4X level 2: 8X level (product dependent)
autoiris	<boolean>	4/4	Enable auto Iris (product dependent)

Group: **audioin_c<0~(n-1)>** for n channel products (capability.audioin>0)

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
source	micin, linein	4/4	micin => use external microphone input linein => use line input
mute	0, 1	4/4	Enable audio mute
gain	1~37	4/4	Gain of input
gain2	1~37	4/4	Gain of input
s<0~(m-1)>_codectype	aac4, gamr	4/4	set audio codec type for input
s<0~(m-1)>_aac4_bitrate	16000,	4/4	set AAC4 bitrate in bps

	32000, 48000, 64000, 96000, 128000		
s<0~(m-1)>_gamr_bitrate	4750, 5150, 5900, 6700, 7400, 7950, 10200, 12200	4/4	set AMR bitrate in bps

Group: **image_c<0~(n-1)>** for n channel products

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
brightness	-5 ~ 5	4/4	Adjust brightness of image according to mode settings.
saturation	-5 ~ 5	4/4	Adjust saturation of image according to mode settings.
contrast	-5 ~ 5	4/4	Adjust contrast of image according to mode settings.
sharpness	-5 ~ 5	4/4	Adjust sharpness of image according to mode settings.
IBPE_edgeenable	<boolean>	4/4	Enable edge enhancement.
IBPE_edgestrength	1 ~ 128	4/4	Adjust edge enhancement strength. 1 is minimum and 128 is maximum.
IBPE_nrenable	<boolean>	4/4	Enable noise reduction.
IBPE_nrmode	1 ~ 3	4/4	Adjust noise reduction mode. 1 => DeGaussian 2 => DeImpulse 3 => DeGaussian + DeImpulse
IBPE_nrstrength	1 ~ 63	4/4	Adjust noise reduction strength. 1 is minimum and 63 is maximum.

Group: **imagepreview_c<0~(n-1)>** for n channel products

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
brightness	-5 ~ 5	4/4	Preview of adjusting brightness of image according to mode settings.
saturation	-5 ~ 5	4/4	Preview of adjusting saturation of image according to mode settings.
contrast	-5 ~ 5	4/4	Preview of adjusting contrast of image according to mode settings.
sharpness	-5 ~ 5	4/4	Preview of adjusting sharpness of image according to mode settings.
IBPE_edgeenable	<boolean>	4/4	Preview of adjusting enabling edge enhancement.
IBPE_edgestrength	1 ~ 128	4/4	Preview of adjusting edge enhancement strength. 1 is minimum and 128 is maximum.
IBPE_nrenable	<boolean>	4/4	Preview of adjusting enabling noise reduction.
IBPE_nrmode	1 ~ 3	4/4	Preview of adjusting noise reduction mode. 1 => DeGaussian 2 => DeImpulse 3 => DeGaussian + DeImpulse
IBPE_nrstrength	1 ~ 63	4/4	Preview of adjusting noise reduction strength. 1 is minimum and 63 is maximum.
videoin_whitebalance	auto, manual	4/4	Preview of adjusting white balance of image according to mode settings
videoin_restoreatwb	0, 1~	4/4	Restore of adjusting white balance of image according to mode settings

Group: **timeshift**, c for n channel products, m is stream number

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	4/4	Enable time shift streaming.
c<0~(n-1)>_s<0~(m-1)>_allow	<boolean>	4/4	Enable time shift streaming for specific stream. (product dependent)

Group: **motion_c<0~(n-1)>** for n channel product

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	4/4	enable motion detection
win_i<0~2>_enable	<boolean>	4/4	enable motion window 1~3
win_i <0~2>_name	string[14]	4/4	name of motion window 1~3
win_i <0~2>_left	0 ~ 320	4/4	Left coordinate of window position.
win_i <0~2>_top	0 ~ 240	4/4	Top coordinate of window position.
win_i <0~2>_width	0 ~ 320	4/4	Width of motion detection window.
win_i<0~2>_height	0 ~ 240	4/4	Height of motion detection window.
win_i<0~2>_objsize	0 ~ 100	4/4	Percent of motion detection window.
win_i<0~2>_sensitivity	0 ~ 100	4/4	Sensitivity of motion detection window.

Group: **motion_ c<0~(n-1)>_profile_i<0~(m-1)>** for n channel, m motion profile product
(capability_nmotionprofile > 0)

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	4/4	enable motion detection
policy	day, night, schedule	4/4	When the condition match the policy, use this profile
begintime	hh:mm	4/4	If choose “schedule” mode as profile policy, the begin time of this profile when enabled
endtime	hh:mm	4/4	If choose “schedule” mode as profile policy, the end time of this profile when enabled
win_i<0~2>_enable	<boolean>	4/4	enable motion window 1~3
win_i <0~2>_name	string[14]	4/4	name of motion window 1~3
win_i <0~2>_left	0 ~ 320	4/4	Left coordinate of window position.
win_i <0~2>_top	0 ~ 240	4/4	Top coordinate of window position.
win_i <0~2>_width	0 ~ 320	4/4	Width of motion detection window.
win_i<0~2>_height	0 ~ 240	4/4	Height of motion detection window.
win_i<0~2>_objsize	0 ~ 100	4/4	Percent of motion detection window.
win_i<0~2>_sensitivity	0 ~ 100	4/4	Sensitivity of motion detection window.

Group: tampering_c<0~(n-1)> for n channel,

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	0	4/4	Enable or disable camera tampering detection
threshold	0 ~ 255	32	4/4	The sensitivity to judge if camera has been tampered 0: lowest sensitivity 255: highest sensitivity
duration	10 ~ 600	10	4/4	Judge camera has been tampered if exceeding this duration

Group: **ddns**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	6/6	Enable or disable the dynamic dns.
provider	Safe100, DyndnsDynamic, DyndnsCustom, TZO, DHS, DynInterfree, CustomSafe100	6/6	Safe100 => safe100.net DyndnsDynamic => dyndns.org (dynamic) DyndnsCustom => dyndns.org (custom) TZO => tzo.com DHS => dhs.org DynInterfree =>dyn-interfree.it CustomSafe100 => Custom server using safe100 method
<provider>_hostname	string[128]	6/6	Your dynamic hostname.
<provider>_usernam eemail	string[64]	6/6	Your user or email to login ddns service provider
<provider>_password key	string[64]	6/6	Your password or key to login ddns service provider
<provider>_serverna me	string[128]	6/6	The server name for safe100. (This field only exists for provider is customsafe100)

Group: **upnppresentation**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	6/6	Enable or disable the UPNP presentation service.

Group: **upnpportforwarding**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	6/6	Enable or disable the UPNP port forwarding service.
upnpnatstatus	0~3	6/7	The status of UpnP port forwarding, used internally. 0 is OK, 1 is FAIL, 2 is no IGD router, 3 is no need to do port forwarding

Group: **syslog**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
enableremotelog	<boolean>	6/6	enable remote log
serverip	<IP address>	6/6	Log server IP address
serverport	514, 1025~65535	6/6	Server port used for log
level	0~7	6/6	The levels to distinguish the importance of information. 0: LOG_EMERG 1: LOG_ALERT 2: LOG_CRIT 3: LOG_ERR 4: LOG_WARNING 5: LOG_NOTICE 6: LOG_INFO 7: LOG_DEBUG

Group: **camctrl_c<0~(n-1)>** for n channel product (capability.ptzenabled)

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
panspeed	-5 ~ 5	1/4	Pan speed
tiltspeed	-5 ~ 5	1/4	Tilt speed
zoomspeed	-5 ~ 5	1/4	Zoom speed
focusspeed	-5 ~ 5	1/4	Auto focus speed
patrolseq	0 ~ 64	1/4	Patrol sequence
patroldwelling	0 ~ 128	1/4	Patrol dwelling time
preset_i<0~19>_name	string[40]	1/4	The name of preset location
preset_i<0~19>_dwelling	0 ~ 255	1/4	The dwelling time of each preset location

uart	0 ~ (m-1), m is uart count	1/4	select correspond uart (capability.nuart>0)
cameraid	0~255	1/4	Camera ID to control external PTZ cameral
isptz	0 ~ 2	1/7	0: disable PTZ commands. 1: enable PTZ commands with PTZ driver. 2: enable PTZ commands with UART tunnel.
disablemdonptz	<boolean>	1/4	disable motion detection on PTZ operation

Group: **uart** (capability.nuart>0) (product dependent)

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
ptzdrivers_i<0~19, 127>_name	string[40]	1/4	The name of the PTZ driver
ptzdrivers_i<0~19, 127>_location	string[128]	1/4	The full path of the PTZ driver
update	1	7/4	update the list of built-in external PTZ drivers
enablehttptunnel	<boolean>	4/4	Enable HTTP tunnel channel to control UART

Group:**uart_i<0~(n-1)>** n is uart port count (capability.nuart>0)

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
baudrate	110,300,600,1200,2400,3600,4800,7200,9600,19200,38400,57600,115200	4/4	set baud rate of COM port
databit	5,6,7,8	4/4	data bits in a character frame
paritybit	none, odd, even	4/4	For error checking
stopbit	1,2	4/4	1 2-1.5 , data bit is 5 2-2
uartmode	rs485, rs232	4/4	rs485 or rs232
customdrvcmd_i<0~9>	string[128]	1/4	PTZ command for custom camera.

speedlink_i<0~4>_name	string[40]	1/4	Additional PTZ command name
speedlink_i<0~4>_cmd	string[128]	1/4	Additional PTZ command list
updatecustomdrvcmd	1	7/4	set this flag to true to apply change of custom command configuration
updatespeedlinkcmd	1	7/4	set this flag to true to apply change of additional PTZ command configuration
ptzdriver	0~19, 127 (custom), 128 (no driver)	4/4	which PTZ driver is used by this COM port

Group: **snmp** (capability.snmp) (product dependent)

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
versions	1 ~ 3	6/6	SNMP version to use.
rocomm	string[14]	6/6	V1, V2c Read only community.
rwcomm	string[14]	6/6	V1, V2c Read write community.
adminauthtype	0 ~ 2	6/6	Authority type for root authentication.
admindpvcy	string[64]	6/6	Root data encryption key.
enableadpvcy	<boolean>	6/6	Enable root data encryption key.
userauthtype	0 ~ 2	6/6	User authority authentication.
userdpvcy	string[64]	6/6	User data encryption key.
enableudpvcy	<boolean>	6/6	Enable user data encryption key.
trapserver	<ip address>, <domain name> [128]	6/6	Trap server
trapcomm	string[14]	6/6	Trap community
objectid	string[40]	6/6	Object ID

Group: **layout** (product dependent)

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
logo_default	<boolean>	1/6	0 => Custom logo 1 => Default logo

logo_link	string[40]	1/6	Hyperlink of the logo
theme_option	1~4	1/6	1~3: One of the default themes 4: Custom definition
theme_color_font	string[7]	1/6	Font color
theme_color_configfont	string[7]	1/6	Font color of configuration area
theme_color_titlefont	string[7]	1/6	Font color of video title
theme_color_controlbackground	string[7]	1/6	Background color of control area
theme_color_configbackground	string[7]	1/6	Background color of configuration area
theme_color_videobackground	string[7]	1/6	Background color of video area
theme_color_case	string[7]	1/6	Frame color

Group: **privacymask_c<0~(n-1)>** for n channel product

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	4/4	Enable the privacy mask
win_i<0~4>_enable	<boolean>	4/4	Enable the privacy mask window
win_i<0~4>_name	string[14]	4/4	The name of privacy mask window
win_i<0~4>_left	0 ~ 320/352	4/4	Left coordinate of window position.
win_i<0~4>_top	0 ~ 240/288	4/4	Top coordinate of window position.
win_i<0~4>_width	0 ~ 320/352	4/4	Width of privacy mask window
win_i<0~4>_height	0 ~ 240/288	4/4	Height of privacy mask window
win_i<0~4>_color	0 ~ 13	4/4	Color of privacy mask window

Group: **capability**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
api_httpversion	0200a	0/7	The HTTP API version.
bootuptime	<positive integer>	0/7	The server bootup time
nir	0, <positive integer>	0/7	number of IR interface
ndi	0, <positive integer>	0/7	number of digital input

ndo	0, <positive integer>	0/7	number of digital output
naudioin	0, <positive integer>	0/7	number of audio input
naudioout	0, <positive integer>	0/7	number of audio output
nvideoin	<positive integer>	0/7	number of video input
nmediastream	<positive integer>	0/7	number of media stream per channel
nvideosetting	<positive integer>	0/7	number of video settings per channel
naudiosetting	<positive integer>	0/7	number of audio settings per channel
nuart	0, <positive integer>	0/7	number of UART interface
nvideoinprofile	0, <positive integer>	0/7	number of sensor profiles
nmotionprofile	0, <positive integer>	0/7	number of motion profiles
ptzenabled	< positive integer >	0/7	An 32-bits integer, each bit can be set separately as follows: Bit 0 => Support camera control function 0(not support), 1(support) Bit 1 => Build-in or external camera. 0(external), 1(build-in) Bit 2 => Support pan operation. 0(not support), 1(support) Bit 3 => Support tilt operation. 0(not support), 1(support) Bit 4 => Support zoom operation. 0(not support), 1(support) Bit 5 => Support focus operation. 0(not support), 1(support) Bit 6 => Support iris operation. 0(not support), 1(support) Bit 7 => External or build-in PT. 0(build-in), 1(external) Bit 8 => Invalidate bit 1 ~ 7. 0(bit 1 ~ 7 are valid), 1(bit 1 ~ 7 are invalid)

			Bit 9 => Reserved bit; Invalidate lens_pan, Lens_tilt, lens_zoon, lens_focus, len_iris. 0(fields are valid), 1(fields are invalid)
eptz	<positive integer>	0/7	A 32-bit integer, each bit can be set separately as follows: Bit 0 => stream 1 supports ePTZ or not. Bit 1 => stream 2 supports ePTZ or not. The rest may be deduced by analogy
protocol_https	<boolean>	0/7	indicate whether to support http over SSL
protocol_rtsp	<boolean>	0/7	indicate whether to support rtsp
protocol_sip	<boolean>	0/7	indicate whether to support sip
protocol_maxconnection	<positive integer>	0/7	The maximum allowed simultaneous connections
protocol_rtp_multicast_ scalable	<boolean>	0/7	indicate whether to support scalable multicast
protocol_rtp_multicast_ backchannel	<boolean>	0/7	indicate whether to support backchannel multicast
protocol_rtp_tcp	<boolean>	0/7	indicate whether to support rtp over tcp
protocol_rtp_http	<boolean>	0/7	indicate whether to support rtp over http
protocol_spush_mjpeg	<boolean>	0/7	indicate whether to support server push motion jpeg
protocol_snmp	<boolean>	0/7	indicate whether to support snmp
protocol_ipv6	<boolean>	0/7	indicate whether to support ipv6
videoin_type	0, 1, 2	0/7	0 => Interlaced CCD 1 => Progressive CCD 2 => CMOS
videoin_resolution	<a list of the available resolution separates by comma)	0/7	available resolutions list
videoin_maxframerate	<a list of the available max frame rate separates by comma>	0/7	available framerate at the videoin_resolution list index

videoin_codec	<a list of the available codec types separaters by comma)	0/7	available codec list
videoout_codec	<a list of the available codec types separaters by comma)	0/7	available codec list
audio_aec	<boolean>	0/7	indicate whether to support acoustic echo cancellation
audio_extmic	<boolean>	0/7	indicate whether to support external microphone input
audio_linein	<boolean>	0/7	indicate whether to support external line input
audio_lineout	<boolean>	0/7	indicate whether to support line output
audio_headphone out	<boolean>	0/7	indicate whether to support headphone output
audioin_codec	<a list of the available codec types separaters by comma)	0/7	available codec list
audioout_codec	<a list of the available codec types separaters by comma)	0/7	available codec list
uart_httptunnel	<boolean>	0/7	Indicate whether to support the http tunnel for uart transfer
camctrl_httptunne l	<boolean>	0/7	Indicate whether to support the http tunnel for camera control
camctrl_privilege	<boolean>	0/7	Indicate whether to support “Manage Privilege” of PTZ control in Security page
transmission_mod e	Tx, Rx, Both	0/7	Indicate what kind of transmission mode the machine used. TX: server, Rx: receiver box, Both: DVR?.
network_wire	<boolean>	0/7	Indicate whether to support the Ethernet
network_wireless	<boolean>	0/7	Indicate whether to support the wireless
wireless_802dot1 1b	<boolean>	0/7	Indicate whether to support the wireless 802.11b+

wireless_802dot11g	<boolean>	0/7	Indicate whether to support the wireless 802.11g
wireless_encrypt_wep	<boolean>	0/7	Indicate whether to support the wireless WEP
wireless_encrypt_wpa	<boolean>	0/7	Indicate whether to support the wireless WPA
wireless_encrypt_wpa2	<boolean>	0/7	Indicate whether to support the wireless WPA2
derivative_brand	<boolean>	0/7	Indicate whether to support upgrade function for the derivative brand. For example, if the value is true, the VVTK product can be upgraded to VVXX. (TCVV<->TCXX is excepted)
evctrlchannel	<boolean>	0/7	Indicate whether to support the http tunnel for event/control transfer
joystick	<boolean>	0/7	Indicate whether to support the joystick control
nanystream	<positive integer>	0/7	number of any media stream per channel

Group: **event_customtaskfile**

PARAMETER	VALUE	SECURITY (get/set)	DESCRIPTION
_i<0~2>_name	string[40]	6/6	Name of custom event task file
_i<0~2>_date	string[20]	6/6	Date of custom event task file
_i<0~2>_time	string[20]	6/6	Time of custom event task file

Group: **event_i<0~2>**

PARAMETER	VALUE	SECURITY (get/set)	DESCRIPTION
name	string[40]	6/6	The identification of this entry
enable	0, 1	6/6	To enable or disable this event.
priority	0, 1, 2	6/6	Indicate the priority of this event. “0” indicates low priority. “1” indicates normal priority. “2” indicates high priority.
delay	1~999	6/6	Delay seconds before detect next event.

trigger	boot, di, motion, seq, visignal	6/6	Indicate the trigger condition. "boot" indicates system boot. "di" indicates digital input. "motion" indicates video motion detection. "seq" indicates periodic condition. "visignal" indicates video input signal loss
di	<integer>	6/6	Indicate which di detected. This field is required when trigger condition is "di". One bit represents one digital input. The LSB indicates DI 0.
mdwin	<integer>	6/6	Indicate which motion detection windows detected. This field is required when trigger condition is "md". One bit represents one window. The LSB indicates the 1^{st} window. For example, to detect the 1^{st} and 3^{rd} windows, set mdwin as 5.
inter	1~999	6/6	Interval of period snapshot in minute. This field is used when trigger condition is "seq".
weekday	<interger>	6/6	Indicate which weekday is scheduled. One bit represents one weekday. The bit0 (LSB) indicates Saturday. The bit1 indicates Friday. The bit2 indicates Thursday. The bit3 indicates Wednesday. The bit4 indicates Tuesday. The bit5 indicates Monday. The bit6 indicates Sunday. For example, to detect events on Friday and Sunday, set weekday as 66.
begintime	hh:mm	6/6	Begin time of weekly schedule.
endtime	hh:mm	6/6	End time of weekly schedule. (00:00 ~ 24:00 means always.)
lowlightcondition	0, 1	6/6	Turn on IR led in some condition: 0: all conditions 1: low light condition

action_do_i<0~(ndo-1)>_enable	0, 1	6/6	To enable or disable trigger digital output.
action_do_i<0~(ndo-1)>_duration	1~999	6/6	The duration of digital output is triggered in seconds.
action_cf_enable	0. 1	6/6	To enable put media on CF.
action_cf_folder	string[128]	6/6	The path to store media.
action_cf_media	NULL, 0~4	6/6	The index of attached media.
action_cf_datefolder	<boolean>	6/6	Enable or disable create folders by date time and hour automatically
action_server_i<0~4>_enable	0, 1	6/6	To enable or disable this server action. The default value is 0.
action_server_i<0~4>_media	NULL, 0~4	6/6	The index of attached media.
action_server_i<0~4>__datefolder	<boolean>	6/6	Enable or disable create folders by date time and hour automatically

Group: **server_i<0~4>**

PARAMETER	VALUE	SECURITY (get/set)	DESCRIPTION
name	string[40]	6/6	The identification of this entry
type	email, ftp, http, ns	6/6	Indicate the server type. “email” is email server. “ftp” is ftp server. “http” is http server. “ns” is network storage.
http_url	string[128]	6/6	The url of http server to upload.
http_username	string[64]	6/6	The username to login in the server.
http_passwd	string[64]	6/6	The password of the user.
ftp_address	string[128]	6/6	The ftp server address
ftp_username	string[64]	6/6	The username to login in the server.
ftp_passwd	string[64]	6/6	The password of the user.
ftp_port	0~65535	6/6	The port to connect the server.
ftp_location	string[128]	6/6	The location to upload or store the media.

ftp_passive	0, 1	6/6	To enable or disable the passive mode. 0 is to disable the passive mode. 1 is to enable the passive mode.
email_address	string[128]	6/6	The email server address
email_sslmode	<boolean>	6/6	To enable or disable the SSL mode 0 is to disable the SSL mode 1 is to enable the SSL mode
email_username	string[64]	6/6	The username to login in the server.
email_httpsmode	0, 1	6/6	Enable support SSL
email_port	0~65535	6/6	The port to connect the server.
email_passwd	string[64]	6/6	The password of the user.
email_senderemail	string[128]	6/6	The email address of sender.
email_recipientemail	string[128]	6/6	The email address of recipient.
ns_location	string[128]	6/6	The location to upload or store the media.
ns_username	string[64]	6/6	The username to login in the server.
ns_passwd	string[64]	6/6	The password of the user.
ns_workgroup	string[64]	6/6	The workgroup for network storage.

Group: **media_i<0~4>**(media_freespace is used internally.)

PARAMETER	VALUE	SECURITY (get/set)	DESCRIPTION
name	string[40]	6/6	The identification of this entry
type	snapshot, systemlog videoclip	6/6	The media type to send to the server or store by the server.
snapshot_source	<integer>	6/6	Indicate the source of media stream. 0 means the first stream. 1 means the second stream and etc. 2 means the third stream and etc. 3 means the fourth stream and etc.
snapshot_prefix	string[16]	6/6	Indicate the prefix of the filename.
snapshot_datesuffix	0, 1	6/6	To add date and time suffix to filename or not. 1 means to add date and time suffix. 0 means not to add it.
snapshot_preevent	0 ~ 7	6/6	It indicates the number of pre-event images.

snapshot_postevent	0 ~ 7	6/6	The number of post-event images.
videoclip_source	<integer>	6/6	Indicate the source of media stream. 0 means the first stream. 1 means the second stream and etc. 2 means the third stream and etc. 3 means the fourth stream and etc.
videoclip_prefix	string[16]	6/6	Indicate the prefix of the filename.
videoclip_preevent	0 ~ 9	6/6	It indicates the time of pre-event recording in seconds.
videoclip_maxduration	1 ~ 10	6/6	The time of maximum duration of one video clip in seconds.
videoclip_maxsize	50 ~ 1500	6/6	The maximum size of one video clip file in Kbytes.

Group: **recording_i**<0~1>

PARAMETER	VALUE	SECURITY (get/set)	DESCRIPTION
name	string[40]	6/6	The identification of this entry
enable	0, 1	6/6	To enable or disable this recoding.
priority	0, 1, 2	6/6	Indicate the priority of this recoding. “0” indicates low priority. “1” indicates normal priority. “2” indicates high priority.
source	<integer>	6/6	Indicate the source of media stream. 0 means the first stream. 1 means the second stream and etc. 2 means the third stream and etc. 3 means the fourth stream and etc.

weekday	<interger>	6/6	Indicate which weekday is scheduled. One bit represents one weekday. The bit0 (LSB) indicates Saturday. The bit1 indicates Friday. The bit2 indicates Thursday. The bit3 indicates Wednesday. The bit4 indicates Tuesday. The bit5 indicates Monday. The bit6 indicates Sunday. For example, to detect events on Friday and Sunday, set weekday as 66.
begintime	hh:mm	6/6	Begin time of weekly schedule.
endtime	hh:mm	6/6	End time of weekly schedule. (00:00~24:00 means always.)
prefix	string[16]	6/6	Indicate the prefix of the filename.
limitsize	0,1	6/6	0: Entire free space mechanism 1: Limit recording size mechanism
cyclesize	20~	6/6	The maximum size for cycle recording in Kbytes when choose limit recording size.
cyclic	0,1	6/6	0: Disable cyclic recording 1: Enable cyclic recording
notify	0,1	6/6	0: Disable recording notification 1: Enable recording notification
notifyserver	0~31	6/6	Indicate which notification server is scheduled. One bit represents one application server (server_i0~i4). The bit0 (LSB) indicates server_i0. The bit1 indicates server_i1. The bit2 indicates server_i2. The bit3 indicates server_i3. The bit4 indicates server_i4. For example, enable server_i0, server_i2 and server_i4 to be notification server. The notifyserver value is 21.
reserveamount	10~	6/6	The reserve amount in Mbytes when choose cyclic recording mechanism.

dest	cf, 0~4	6/6	The destination to store the recording data. “cf” means CF card. “0~4” means the index of network storage.
cffolder	string[128]	6/6	folder name.

Group: **path**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
encoder1_start	<boolean>	7/7	Specify the http push server is active for stream 1
encoder2_start	<boolean>	7/7	Specify the http push server is active for stream 2

Group: **https** (product dependent)

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
connect	1025 ~ 65535	7/7	Specify the stunnel connect port
enable	<boolean>	6/6	To enable or disable this secure http
policy	<Boolean>	6/6	If the value is 1, it will force http connection redirect to https connection
method	auto, manual, install	6/6	auto => Create self-signed certificate automatically manual => Create self-signed certificate manually install => Create certificate request and install
status	-2 ~ 1	6/6	Specify the https status. -2=>invalid public key -1=>waiting for certificated 0=>not installed 1=>active
countryname	string[2]	6/6	country name in certificate information
stateorprovincename	string[128]	6/6	state or province name in in certificate information
localityname	string[128]	6/6	the locality name in certificate information
organizationname	string[64]	6/6	organization naem in certificate information
unit	string[32]	6/6	organizational unit name in certificate

			information
commonname	string[64]	6/6	common name in certificate information
validdays	0 ~ 9999	6/6	certificatation valid period

Group: **disk_i<0~(n-1)>** n is the total number of storage devices.

PARAMETER	VALUE	SECURITY (get/set)	DESCRIPTION
name	string[16]	6/6	Disk name.
cyclic_enabled	<boolean>	6/6	Enable cyclic storage method.
autocleanup_enabled	<boolean>	6/6	Enable automatic clean up method. Expired and not locked media files will be deleted.
autocleanup_maxage	<positive integer>	6/6	To specify the expired days for automatic clean up.

Group: **roi_c<0~(n-1)>** for n channel product, and m is the number of streams which support ROI.

PARAMETER	VALUE	SECURITY (get/set)	DESCRIPTION
s<0~(m-1>_home	<coordinate>	6/6	ROI left-top corner coordinate.
s<0~(m-1>_size	<window size>	6/6	ROI width and height.

Group: **eptz_c<0~(n-1)>** for n channel product.

PARAMETER	VALUE	SECURITY (get/set)	DESCRIPTION
osdzoom	<boolean>	1/4	Indicates multiple of zoom in is “on-screen display” or not
smooth	<boolean>	1/4	Indicates ePTZ is smooth or not.
tiltspeed	-5 ~ 5	1/7	Tilt speed (It should be set by eCamCtrl.cgi rather than by setparam.cgi.)
panspeed	-5 ~ 5	1/7	Pan speed (It should be set by eCamCtrl.cgi rather than by setparam.cgi.)
zoomspeed	-5 ~ 5	1/7	Zoom speed (It should be set by eCamCtrl.cgi rather than by setparam.cgi.)

autospeed	1 ~ 5	1/7	Auto pan/patrol speed (It should be set by eCamCtrl.cgi rather than by setparam.cgi.)

Group: **eptz_c<0~(n-1)>_s<0~(m-1)>** for n channel product. and m is the number of streams which support ePTZ.

PARAMETER	VALUE	SECURITY (get/set)	DESCRIPTION
patrolseq	string[120]	1/4	The indexes of patrol points, separated by ","
patroldwelling	string[160]	1/4	The dwelling time of each patrol point, separated by ","
i<0~19>_name	string[40]	1/7	Name of ePTZ preset. (It should be set by eCamCtrl.cgi rather than by setparam.cgi.)
i<0~19>_pos	<coordinate>	1/7	Left-top corner coordinate of the preset. (It should be set by eCamCtrl.cgi rather than by setparam.cgi.)
i<0~19>_size	<window size>	1/7	Width and height of the preset. (It should be set by eCamCtrl.cgi rather than by setparam.cgi.)

Drive the digital output

Note: This request requires the privilege of viewer.

Method: GET/POST

Syntax:

```
http://<servername>/cgi-bin/dido/setdo.cgi?do1=<state>[&do2=<state>]
[&do3=<state>][&do4=<state>][&return=<return page>]
```

Where state is 0, 1. "0" means inactive or normal state while "1" means active or triggered state.

PARAMETER	VALUE	DESCRIPTION
do<num>	0, 1	0 – inactive, normal state 1 – active, triggered state
return	*<return page>*	Redirect to the page *<return page>* after the parameter is assigned. The *<return page>* can be a full URL path or relative

		path according to the current path. If you omit this parameter, it will redirect to an empty page.

Example: Drive the digital output 1 to triggered state and redirect to an empty page

http://myserver/cgi-bin/dido/setdo.cgi?do1=1

Query status of the digital input

Note: This request requires the privilege of viewer.

Method: GET/POST

Syntax:

http://<*servername*>/cgi-bin/dido/getdi.cgi?[di0][&di1][&di2][&di3]

If no parameter is specified, all the status of digital input will be returned.

Return:

HTTP/1.0 200 OK\r\n Content-
Type: text/plain\r\n Content-Length:
<*length*>\r\n
\r\n *[di0=<state>]*\r\n
[di1=<state>]\r\n
[di2=<state>]\r\n
[di3=<state>]\r\n
where <*state*> can be 0 or 1.

Example: Query the status of digital input 1

Request:
http://myserver/cgi-bin/dido/getdi.cgi?di1

Response:
HTTP/1.0 200 OK\r\n Content-
Type: text/plain\r\n Content-
Length: 7\r\n
\r\n
di1=1\r\n

Query status of the digital output

Note: This request requires the privilege of viewer.

Method: GET/POST

Syntax:

http://<*servername*>/cgi-bin/dido/getdo.cgi?[do0][&do1][&do2][&do3]

If no parameter is specified, all the status of digital output will be returned.

Return:

HTTP/1.0 200 OK\r\n Content- Type: text/plain\r\n Content-Length: <*length*>\r\n \r\n *[do0=<state>]\r\n* *[do1=<state>]\r\n* *[do2=<state>]\r\n* *[do3=<state>]\r\n* where <*state*> can be 0 or 1.

Example: Query the status of digital output 1

Request:

http://myserver/cgi-bin/dido/getdo.cgi?do1

Response:

HTTP/1.0 200 OK\r\n Content-

Type: text/plain\r\n Content-

Length: 7\r\n

\r\n

do1=1\r\n

Capture single snapshot

Note: This request require normal user privilege

Method: GET/POST

Syntax:

http://<*servername*>/cgi-bin/viewer/video.jpg?[channel=<value>][&resolution=<value>]
[&quality=<value>]

If the user requests the size larger than all stream setting on the server, this request will failed!

PARAMETER	VALUE	DEFAULT	DESCRIPTION
channel	0~(n-1)	0	the channel number of video source
resolution	*<available resolution>*	0	The resolution of image
quality	*1~5*	3	The quality of image

Server will return the most up-to-date snapshot of selected channel and stream in JPEG format. The size and quality of image will be set according to the video settings on the server.

Return:

HTTP/1.0 200 OK\r\n
Content-Type: image/jpeg\r\n
[Content-Length: <image size>\r\n]

<binary JPEG image data>

Account management

Note: This request requires administrator privilege

Method: GET/POST

Syntax:

http://<*servername*>/cgi-bin/admin/editaccount.cgi?
method=<value>&username=<*name*>[&userpass=<*value*>][&privilege=<*value*>]
[&privilege=<value>][…][&return=<*return page*>]

PARAMETER	VALUE	DESCRIPTION
method	Add	Add an account to server. When using this method, “username” field is necessary. It will use default value of other fields if not specified.

	Delete	Remove an account from server. When using this method, "username" field is necessary, and others are ignored.
	edit	Modify the account password and privilege. When using this method, "username" field is necessary, and other fields are optional. If not specified, it will keep original settings.
username	<name>	The name of user to add, delete or edit
userpass	<value>	The password of new user to add or that of old user to modify. The default value is an empty string.
privilege	<value>	The privilege of user to add or to modify.
	viewer	viewer's privilege
	operator	operator's privilege
	admin	administrator's privilege
return	<return page>	Redirect to the page *<return page>* after the parameter is assigned. The *<return page>* can be a full URL path or relative path according to the current path. If you omit this parameter, it will redirect to an empty page.

System logs

Note: This request require administrator privilege

Method: GET/POST

Syntax:

http://<*servername*>/cgi-bin/admin/syslog.cgi

Server will return the up-to-date system log.

Return:

```
HTTP/1.0 200 OK\r\n
Content-Type: text/plain\r\n
Content-Length: <syslog length>\r\n
\r\n
<system log information>\r\n
```

Configuration file (optional)

Note: This request requires administrator privilege

Method: GET/POST

Syntax:

http://<*servername*>/cgi-bin/admin/configfile.cgi?[format=<value>]

Server will return the up-to-date configuration file.

PARAMETER	VALUE	DEFAULT	DESCRIPTION
format	xml	xml	the format for config file.

Return:

```
HTTP/1.0 200 OK\r\n
Content-Type: text/plain\r\n
Content-Length: <configuration file length>\r\n
\r\n
<configuration data>\r\n
```

Upgrade firmware

Note: This request requires administrator privilege

Method: POST

Syntax:

http://<*servername*>/cgi-bin/admin/upgrade.cgi

Post data:

```
fimage=<file name>[&return=<return page>]\r\n
\r\n
<multipart encoded form data>
```

Server will accept the upload file named <file name> to be upgraded the firmware and return with <return page> if indicated.

Camera Control (capability.ptzenabled=1)

Note: This request requires privilege of viewer

Method: GET/POST

Syntax:

http://<*servername*>/cgi-bin/viewer/camctrl.cgi?[channel=<value>][&camid=<value>][&move=<valu e>]
[&focus=<value>][&iris=<value>][&speedpan=<value>][&speedtilt=<value>][&speedzoom=<value>]
[&speedapp=<value>][&auto=<value>][&zoom=<value>][&zooming=<value>][&speedlink=<value>]
[&vx=<value>&vy=<value>&vs=<value>] [&return=<*return page*>]

PARAMETER	VALUE	DESCRIPTION
channel	<0~(n-1)>	Channel of video source
camid	0,<positive integer>	Camera ID
move	home	Move to camera to home position
	up	Move camera up
	down	Move camera down
	left	Move camera left
	right	Move camera right
speedpan	-5 ~ 5	Set the pan speed
speedtilt	-5 ~ 5	Set the tilt speed
speedzoom	-5 ~ 5	Set the zoom speed
speedapp	-5 ~ 5	Set the auto pan/patrol speed
auto	pan	Auto pan
	patrol	Auto patrol
	stop	Stop camera
zoom	wide	To zoom for larger view with current speed
	tele	To zoom for farer view with current speed
	stop	To stop zoom
zooming	wide	To zoom without stop for larger view with current speed

	tele	To zoom without stop for farer view with current speed
vx	<integer , excluding 0>	The slope of movement = vy/vx, used for joystick control.
vy	<integer>	
vs	0 ~ 7	Set the speed of movement, “0” means stop.
focus	auto	To do auto focus
	far	To focus on farer distance
	near	To focus on nearer distance
iris	auto	Let the Network Camera control iris size
	open	Manually control the iris for bigger size
	close	Manually control the iris for smaller size
speedlink	0 ~ 4	Issue speed link command.
return	<return page>	Redirect to the page <*return page*> after the parameter is assigned. The <*return page*> can be a full URL path or relative path according to the current path. If you omit this parameter, it will redirect to an empty page.

ePTZ Camera Control

Note: This request requires camctrl privileges.

Method: GET/POST

Syntax:

```
http://<servername>/cgi-bin/camctrl/eCamCtrl.cgi?channel=<value>&stream=<value>
[&move=<value>][&auto=<value>][&zoom=<value>] [&zooming=<value>&zs=<value>]
[&vx=<value>&vy=<value>&vs=<value>]
[&speedpan=<value>][&speedtilt=<value>][&speedzoom=<value>][&speedapp=<value>] [&return=<return
page>]
```

PARAMETER	VALUE	DESCRIPTION
channel	<0~(n-1)>	Channel of video source.
stream	<0~(m-1)>	Stream.

move	home	Move to home ROI.
	up	Move up.
	down	Move down.
	left	Move left.
	right	Move right.
auto	pan	Auto pan.
	patrol	Auto patrol.
	stop	Stop auto pan/patrol.
zoom	wide	Zoom larger view with current speed.
	tele	Zoom further with current speed.
zooming	wide or tele	Zoom without stopping for larger view or further view with zs speed, used for joystick control.
zs	0 ~ 6	Set the speed of zooming, “0” means stop.
vx	<integer>	The direction of movement, used for joystick control.
vy	<integer>	
vs	0 ~ 7	Set the speed of movement, “0” means stop.
speedpan	-5 ~ 5	Set the pan speed.
speedtilt	-5 ~ 5	Set the tilt speed.
speedzoom	-5 ~ 5	Set the zoom speed.
speedapp	1 ~ 5	Set the auto pan/patrol speed.
return	<return page>	Redirect to the page *<return page>* after the parameter is assigned. The *<return page>* can be a full URL path or relative path according to the current path.

Recall (capability.ptzenabled=1)

Note: This request requires privilege of viewer

Method: GET

Syntax:

http://<*servername*>/cgi-bin/viewer/recall.cgi?

```
recall=<value>[&channel=<value>][&return=<return page>]
```

PARAMETER	VALUE	DESCRIPTION
recall	Text string less than 30 characters	One of the present positions to recall.
channel	<0~(n-1)>	channel of video source
return	*<return page>*	Redirect to the page *<return page>* after the parameter is assigned. The *<return page>* can be a full URL path or relative path according to the current path. If you omit this parameter, it will redirect to an empty page.

ePTZ Recall

Note: This request requires camctrl privileges.

Method: GET/POST

Syntax:

```
http://<servername>/cgi-bin/camctrl/eRecall.cgi?channel=<value>&stream=<value>&
recall=<value>[&return=<return page>]
```

PARAMETER	VALUE	DESCRIPTION
channel	<0~(n-1)>	Channel of the video source.
stream	<0~(m-1)>	Stream.
recall	Text string less than 40 characters	One of the present positions to recall.
return	*<return page>*	Redirect to the page *<return page>* after the parameter is assigned. The *<return page>* can be a full URL path or relative path according to the current path.

Preset Locations (capability.ptzenabled=1)

Note: This request requires operator privilege

Method: GET/POST

Syntax:

http://<*servername*>/cgi-bin/operator/preset.cgi?[channel=<value>]
[&addpos=<value>][&delpos=<value>][&return=<*return page*>]

PARAMETER	VALUE	DESCRIPTION
addpos	<Text string less than 30 characters>	Add one preset location to preset list.
channel	<0~(n-1)>	channel of video source
delpos	<Text string less than 30 characters>	Delete preset location from preset list.
return	<*return page*>	Redirect to the page <*return page*> after the parameter is assigned. The <*return page*> can be a full URL path or relative path according to the current path. If you omit this parameter, it will redirect to an empty page.

ePTZ Preset Locations

Note: This request requires Operator privileges.

Method: GET/POST

Syntax:

http://<*servername*>/cgi-bin/operator/ePreset.cgi?channel=<value>&stream=<value>
[&addpos=<value>][&delpos=<value>][&return=<*return page*>]

PARAMETER	VALUE	DESCRIPTION
channel	<0~(n-1)>	Channel of the video source.
stream	<0~(m-1)>	Stream.
addpos	<Text string less than 40 characters>	Add one preset location to the preset list.
delpos	<Text string less than 40 characters>	Delete preset location from the preset list.

return	*<return page>*	Redirect to the page *<return page>* after the parameter is assigned. The *<return page>* can be a full URL path or relative path according to the current path.

System Information

Note: This request requires normal user privilege (obsolete)

Method: GET/POST

Syntax:

http://<*servername*>/cgi-bin/sysinfo.cgi

Server will return the system information. In HTTP API version 2, the CapVersion will be 0200. All the fields in the previous version (0100) is obsolete. Please use "getparam.cgi?capability" instead.

Return:

```
HTTP/1.0 200 OK\r\n
Content-Type: text/plain\r\n
Content-Length: <system information length>\r\n
\r\n
Model=<model name of server>\r\n
CapVersion=0200\r\n
```

PARAMETER(supported capability version)	VALUE	DESCRIPTION
Model	system.firmwareversion	Model name of server. Ex:IP3133-VVTK-0100a
CapVersion	*MMmm, MM is major version from 00 ~ 99 mm is minor version from 00 ~ 99* *ex: 0100*	The capability field version

IP filtering

Note: This request requires administrator access privilege

Method: GET/POST

Syntax:

```
http://<servername>/cgi-bin/admin/ipfilter.cgi?
method=<value>&[start=<ipaddress>&end=<ipaddress>][&index=<value>]
[&return=<return page>]
```

PARAMETER	VALUE	DESCRIPTION
Method	addallow	Add a set of allow IP address range to server. Start and end parameters must be specified. If the index parameter is specified, it will try to add starting from index position.
	adddeny	Add a set of deny IP address range to server. Start and end parameters must be specified. If the index parameter is specified, it will try to add starting from index position.
	deleteallow	Remove a set of allow IP address range from server. If start and end parameters are specified, it will try to remove the matched IP address. If index is specified, it will try to remove the address from given index position. [start, end] parameters have higher priority then the [index] parameter.
	deletedeny	Remove a set of deny IP address range from server. If start and end parameters are specified, it will try to remove the matched IP address. If index is specified, it will try to remove the address from given index position. [start, end] parameters have higher priority then the [index] parameter.
start	<ip address>	The start IP address to add or to delete.
end	<ip address>	The end IP address to add or to delete.
index	<value>	The start position to add or to delete.
return	<return page>	Redirect to the page *<return page>* after the parameter is assigned. The *<return page>* can be a full URL path or relative path according to the current path. If you omit this parameter, it will redirect to an empty page.

UART HTTP tunnel channel (capability.nuart>0)

Note: This request requires operator privilege

Method: GET and POST

Syntax:

```
http://<servername>/cgi-bin/operator/uartchannel.cgi?[channel=<value>]
------------------------------------------------------------------------ GET /cgi-
bin/operator/uartchannel.cgi?[channel=<value>]
x-sessioncookie: string[22]
accept: application/x-vvtk-tunnelled
pragma: no-cache
cache-control: no-cache

------------------------------------------------------------------------ POST /cgi-
bin/operator/uartchannel.cgi
x-sessioncookie: string[22]
content-type: application/x-vvtk-tunnelled pragma
: no-cache
cache-control : no-cache
content-length: 32767
expires: Sun, 9 Jam 1972 00:00:00 GMT
```

User must use GET and POST to establish two channels for downstream and upstream. The x-sessioncookie in the GET and POST should be the same to be recognized as a pair for one session. The contents of upstream should be base64 encoded to be able to pass through some proxy server.

This channel will help to transfer the raw data of UART over network.

PARAMETER	VALUE	DESCRIPTION
channel	0 ~ (n-1)	The channel number of UART.

Event/Control HTTP tunnel channel

Note: This request requires admin privilege

Method: GET and POST

Syntax:

```
http://<servername>/cgi-bin/admin/ctrlevent.cgi
------------------------------------------------------------------------ GET /cgi-
bin/admin/ctrlevent.cgi
```

```
x-sessioncookie: string[22]
accept: application/x-vvtk-tunnelled
pragma: no-cache
cache-control: no-cache

---------------------------------------------------------------------- POST /cgi-
bin/admin/ ctrlevent.cgi
x-sessioncookie: string[22]
content-type: application/x-vvtk-tunnelled pragma
: no-cache
cache-control : no-cache
content-length: 32767
expires: Sun, 9 Jam 1972 00:00:00 GMT
```

User must use GET and POST to establish two channels for downstream and upstream. The x-sessioncookie in the GET and POST should be the same to be recognized as a pair for one session. The contents of upstream should be base64 encoded to be able to pass through some proxy server.

This channel will help to do real-time event notification and control. The event and control format are described in another document.

Get SDP of Streamings

Note: This request requires viewer access privilege
Method: GET/POST

Syntax:

```
http://<servername>/<network_rtsp_s<0~m-1>_accessname>
```

“m” is the stream number.
“network_accessname_<0~(m-1)>” is the accessname for stream “1” to stream “m”. Please refer to the “subgroup of network: rtsp” for setting the accessname of SDP. You can get the SDP by HTTP GET method.

Open the network streamings

Note: This request requires viewer access privilege

Syntax:

For http push server (mjpeg):

http://<*servername*>/<network_http_s<0~m-1>_accessname>

For rtsp (mp4), user needs to input the url below for a rtsp compatible player.

rtsp://<*servername*>/<network_rtsp_s<0~m-1>_accessname>

"m" is the stream number.

For detailed streaming protocol, please refer to "control signaling" and "data format" documents.

Senddata (capability.nuart>0)

Note: This request requires privilege of viewer

Method: GET/POST

Syntax:

http://<*servername*>/cgi-bin/viewer/senddata.cgi? [com=<value>][&data=<value>][&flush=<value>]
[&wait=<value>] [&read=<value>]

PARAMETER	VALUE	DESCRIPTION
com	1 ~ <max. com port number>	The target com/rs485 port number
data	<hex decimal data>[,<hex decimal data>]	The <hex decimal data> is s series of digit within 0 ~ 9, A ~ F. Each comma separates the commands by 200 milliseconds.
flush	yes,no	yes: receive data buffer of COM port will be cleared before read. no: do not clear the receive data buffer.
wait	*1 ~ 65535*	wait time in milliseconds before read data
read	*1 ~ 128*	the data length in bytes to read. The read data will be in return

		page.

Return:

```
HTTP/1.0 200 OK\r\n
Content-Type: text/plain\r\n
Content-Length: <system information length>\r\n
\r\n
<hex decimal data>\r\n
```

Where is hex decimal data is a series of digit within 0 ~ 9, A ~ F

Storage managements (capability.storage.dbenabled=1)

Note: This request requires administrator privileges.

Method: GET and POST

Syntax:

```
http://<servername>/cgi-bin/admin/lsctrl.cgi?cmd=<cmd_type>[&<parameter>=<value>…]
```

The commands usage and their input arguments are as follows.

PARAMETER	VALUE	DESCRIPTION
cmd_type	<string>	Required. Command to be executed, including *search*, *insert*, *delete*, *update*, and *queryStatus*.

Command: **search**

PARAMETER	VALUE	DESCRIPTION
label	<integer primary key>	Optional. The integer primary key column will automatically be assigned a unique integer.
triggerType	<text>	Optional. Indicate the event trigger type. Please embrace your input value with single quotes. Ex. mediaType='motion' Support trigger types are product dependent.
mediaType	<text>	Optional. Indicate the file media type.

		Please embrace your input value with single quotes. Ex. mediaType='videoclip' Support trigger types are product dependent.
destPath	<text>	Optional. Indicate the file location in camera. Please embrace your input value with single quotes. Ex. destPath ='/mnt/auto/CF/NCMF/abc.mp4'
resolution	<text>	Optional. Indicate the media file resolution. Please embrace your input value with single quotes. Ex. resolution='800x600'
isLocked	<boolean>	Optional. Indicate if the file is locked or not. 0: file is not locked. 1: file is locked. A locked file would not be removed from UI or cyclic storage.
triggerTime	<text>	Optional. Indicate the event trigger time. (not the file created time) Format is "YYYY-MM-DD HH:MM:SS" Please embrace your input value with single quotes. Ex. triggerTime='2008-01-01 00:00:00' If you want to search for a time period, please apply "TO" operation. Ex. triggerTime='2008-01-01 00:00:00'+TO+'2008-01-01 23:59:59' is to search for records from the start of Jan 1st 2008 to the end of Jan 1st 2008.
limit	<positive integer>	Optional. Limit the maximum number of returned search records.
offset	<positive integer>	Optional. Specifies how many rows to skip at the beginning of the matched records. Note that the offset keyword is used after limit keyword.

To increase the flexibility of search command, you may use "OR" connectors for logical "OR" search operations. Moreover, to search for a specific time period, you can use "TO" connector.

Ex. To search records triggered by motion or di or sequential and also triggered between 2008-01-01 00:00:00 and 2008-01-01 23:59:59.

```
http://<servername>/cgi-bin/admin/lsctrl.cgi?cmd=search&triggerType='motion'+OR+'di'+OR+'seq'&tr
iggerTime='2008-01-01 00:00:00'+TO+'2008-01-01 23:59:59'
```

Command: **delete**

PARAMETER	VALUE	DESCRIPTION
label	<integer primary key>	Required. Identify the designated record. Ex. label=1

Ex. Delete records whose key numbers are 1, 4, and 8.

```
http://<servername>/cgi-bin/admin/lsctrl.cgi?cmd=delete&label=1&label=4&label=8
```

Command: **update**

PARAMETER	VALUE	DESCRIPTION
label	<integer primary key>	Required. Identify the designated record. Ex. label=1
isLocked	<boolean>	Required. Indicate if the file is locked or not.

Ex. Update records whose key numbers are 1 and 5 to be locked status.

```
http://<servername>/cgi-bin/admin/lsctrl.cgi?cmd=update&isLocked=1&label=1&label=5
```

Ex. Update records whose key numbers are 2 and 3 to be unlocked status.

```
http://<servername>/cgi-bin/admin/lsctrl.cgi?cmd=update&isLocked=0&label=2&label=3
```

Command: queryStatus

PARAMETER	VALUE	DESCRIPTION
retType	xml or javascript	Optional. Ex. retype=javascript The default return message is in XML format.

Ex. Query local storage status and call for javascript format return message.

```
http://<servername>/cgi-bin/admin/lsctrl.cgi?cmd=queryStatus&retType=javascript
```

(D) Impressum

Diese Bedienungsanleitung entspricht dem technischen Stand bei Drucklegung.
Änderung in Technik und Ausstattung vorbehalten.

(GB) Imprint

The operating instructions reflect the current technical specifications at the time of print.
We reserve the right to change the technical or physical specifications.

(F) Note de l'éditeur

Cette notice est conforme à la règlementation en vigueur lors de l'impression. Données techniques et conditionnement soumis à modifications sans aucun préalable.

(NL) Impressum

Deze gebrujiksaanwijzing voldoet aan de technische eisen bij het ter perse gaan.
Wijzigingen in techniek en uitrusting voorbehouden.

(DK) Redaktionel note

Denne brugervejledning reflekterer de kendte til dato tekniske specifikationer. Vi forbeholder os retten til at ændre frit og uden forudgående advisering.